Information Security, Privacy, and Compliance Models for Cloud Computing Services

by

Fahad F. Alruwaili
Bachelor of Science, King Fahd University of Petroleum and Minerals, 2002
Master of Science, DePaul University, 2008
Master of Science, Claremont Graduate University, 2011

A Dissertation Submitted in Partial Fulfillment
of the Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Electrical and Computer Engineering

© Fahad F. Alruwaili, 2016
University of Victoria

All rights reserved. This dissertation may not be reproduced in whole or in part, by photocopy or other means, without the permission of the author.

Information Security, Privacy, and Compliance Models for Cloud Computing Services

by

Fahad F. Alruwaili
Bachelor of Science, King Fahd University of Petroleum and Minerals, 2002
Master of Science, DePaul University, 2008
Master of Science, Claremont Graduate University, 2011

Supervisory Committee

Dr. T. Aaron Gulliver, Supervisor
(Department of Electrical and Computer Engineering)

Dr. Daler N. Rakhmatov, Departmental Member
(Department of Electrical and Computer Engineering)

Dr. Sudhakar Ganti, Outside Member
(Department of Computer Science)

Supervisory Committee

Dr. T. Aaron Gulliver, Supervisor
(Department of Electrical and Computer Engineering)

Dr. Daler N. Rakhmatov, Departmental Member
(Department of Electrical and Computer Engineering)

Dr. Sudhakar Ganti, Outside Member
(Department of Computer Science)

Abstract

The recent emergence and rapid advancement of Cloud Computing (CC) infrastructure and services have made outsourcing Information Technology (IT) and digital services to Cloud Providers (CPs) attractive. Cloud offerings enable reduction in IT resources (hardware, software, services, support, and staffing), and provide flexibility and agility in resource allocation, data and resource delivery, fault-tolerance, and scalability. However, the current standards and guidelines adopted by many CPs are tailored to address functionality (such as availability, speed, and utilization) and design requirements (such as integration), rather than protection against cyber-attacks and associated security issues. In order to achieve sustainable trust for cloud services with minimal risks and impact on cloud customers, appropriate cloud information security models are required. The research described in this dissertation details the processes adopted for the development and implementation of an integrated information security cloud based approach to cloud service models. This involves detailed investigation into the inherent information security deficiencies identified in the existing cloud service models, service agreements, and compliance issues. The research conducted was a multidisciplinary in nature, with detailed investigations on factors such as people, technology, security, privacy, and compliance involved in cloud risk assessment to ensure all aspects are addressed in holistic and well-structured models.

The primary research objectives for this dissertation are investigated through a series of scientific papers centered on these key research disciplines. The assessment of information security, privacy, and compliance implementations in a cloud environment is described in Chapters two, three, four, and five. Paper 1 *(CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services)* outlines a framework for detecting and preventing known and zero-day threats targeting cloud computing networks. This framework forms the basis for implementing enhanced threat detection and prevention via behavioral and anomaly data analysis. Paper 2 *(A Trusted CCIPS Framework)* extends the work of cooperative intrusion detection and prevention to enable trusted delivery of cloud services. The trusted CCIPS model details and justifies the multi-layer approach to enhance the performance and efficiency of detecting and preventing cloud threats. Paper 3 *(SOCaaS: Security Operations Center as a Service for Cloud Computing Environments*) describes the need for a trusted third party to perform real-time monitoring of cloud services to ensure compliance with security requirements by suggesting a security operations center system architecture. Paper 4 *(SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services)* identifies the necessary cloud security and privacy controls that need to be addressed in the contractual agreements, i.e. service level agreements (SLAs), between CPs and their customers.

Papers five, six, seven, and eight (Chapters 6 – 9) focus on addressing and reducing the risk issues resulting from poor assessment to the adoption of cloud services and the factors that influence such as migration. The investigation of cloud-specific information security risk management and migration readiness frameworks, detailed in Paper 5 *(An Effective Risk Management Framework for Cloud Computing Services)* and Paper 6 *(Information Security, Privacy, and Compliance Readiness Model)* was achieved through extensive consideration of all possible factors obtained from different studies. An analysis of the results indicates that several key factors, including risk tolerance, can significantly influence the migration decision to cloud technology. An additional issue found during this research in assessing the readiness of an organization to move to the cloud is the necessity to ensure that the cloud service provider is actually with

information security, privacy, and compliance (ISPC) requirements. This investigation is extended in Paper 7 *(A Practical Life Cycle Approach for Cloud based Information Security)* to include the six phases of creating proactive cloud information security systems beginning with initial design, through the development, implementation, operations and maintenance. The inherent difficulty in identifying ISPC compliant cloud technology is resolved by employing a tracking method, namely the eligibility and verification system presented in Paper 8 *(Cloud Services Information Security and Privacy Eligibility and Verification System).*

Finally, Paper 9 *(A Case Study of Migration to a Compliant Cloud Technology)* describes the actual implementation of the proposed frameworks and models to help the decision making process faced by the Saudi financial agency in migrating their IT services to the cloud. Together these models and frameworks suggest that the threats and risks associated with cloud services are continuously changing and more importantly, increasing in complexity and sophistication. They contribute to making stronger cloud based information security, privacy, and compliance technological frameworks. The outcomes obtained significantly contribute to best practices in ensuring information security controls are addressed, monitoring, enforced, and compliant with relevant regulations.

List of Publications by Candidate

Published Journal Papers

[1]. F. F. Alruwaili and T. A. Gulliver, "CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services," *International Journal of Latest Trends in Computing*, **Vol. 4, No. 4**, pp. 151-158, December 2013.

[2]. F. F. Alruwaili and T. A. Gulliver, "Trusted CCIPS: A Trust Security Model for Cloud Services Based on a Collaborative Intrusion Detection and Prevention Framework," *International Journal of Latest Trends in Computing*, **Vol. 5, No. 1**, pp. 162-171, March 2014.

[3]. F. F. Alruwaili and T. A. Gulliver, "SOCaaS: Security Operations Center as a Service for Cloud Computing Environment," *International Journal of Cloud Computing and Services Science*, **Vol. 3, No. 2**, pp. 87-96, April 2014.

[4]. F. F. Alruwaili and T. A. Gulliver, "SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services," *International Journal of Cloud Computing and Services Science*, **Vol. 3, No. 4**, August 2014.

[5]. F. F. Alruwaili and T. A. Gulliver, "Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services," *International Journal of Computer Communications and Networks*, **Vol. 1, No. 2**, September 2014.

[6]. F. F. Alruwaili and T. A. Gulliver, "ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services," *International Journal of Future Generation Distributed Systems*, **Vol. 4, No. 4**, December 2014.

[7]. F. F. Alruwaili and T. A. Gulliver, "SecSDLC: A Practical Life Cycle Approach for Cloud-based Information Security," *International Journal of Research in Computer and Communication Technology*, **Vol. 4, No. 2**, February 2015.

[8]. F. F. Alruwaili and T. A. Gulliver, "EVS: Cloud Services Information Security and Privacy Eligibility and Verification System," *International Journal of Research in Computer and Communication Technology*, **Vol. 4, No. 12,** December 2015.

[9]. F. F. Alruwaili and T. A. Gulliver, "Secure Cloud Migration: A Case Study of Migration to a Compliant Cloud Technology," *Submitted to International Journal of Research in Computer and Communication Technology*.

Table of Contents

Supervisory Committee ..... **ii**

Abstract ..... **iii**

List of Publications by Candidate ..... **vi**

Table of Contents ..... **vii**

List of Abbreviations ..... **xi**

List of Tables ..... **xiv**

List of Figures ..... **xv**

Acknowledgments ..... **xvi**

Dedication ..... **xvii**

Introduction **1**
- Background 1
- Research Motivations 5
- Research Methodology 8
- Linkage of Scientific Papers 11

CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services **15**
- Abstract 16
- Introduction 16
- Background and Related Work 17
- Design Objectives 18
- The Cooperative Cloud Intrusion Prevention Framework 19
- Discussion 21
- Conclusion 22
- References 22

Trusted CCIPS: A Trust Security Model for Cloud Services Based on a Collaborative Intrusion Detection and Prevention Framework **24**
- Abstract 25
- Introduction 25
- Cloud Customer Requirements and Motivation 27
- Problem Analysis 27
- Related Work 28
- Objectives 28
- Trusted CCIPS 28
  - Trust Definition 28
  - Scalable Cloud Cooperative Intrusion Prevention (CCIPS) Architecture 29
  - Socio-Technical Systems 29

The Trusted CCIPS Model 30
The Trust Model Structure 32
Discussion 33
Conclusion 34
References 34

SOCaaS: Security Operations Center as a Service for Cloud Computing Environments 36
Abstract 37
Introduction 37
The SOCaaS Concept 38
Related Work 39
Objectives 40
Security Operation Center as a Service (SOCaaS) 40
Event Definition 40
SOCaaS Operational Process 41
SOCaaS Framework 41
Discussion 43
Conclusion 45
References 45

SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services 47
Abstract 48
Introduction 48
Motivation and Customer Requirements 49
Related Work 49
Objectives 50
The Secure Service Level Agreement (SecSLA) 50
SLA and SecSLA Definitions 50
The SecSLA Concept 50
The SecSLA Taxonomy Matrix for Cloud Security and Privacy Controls 51
The SecSLA Control Provisioning Negotiation Process 52
The SecSLA Framework 53
Discussion 56
Conclusion 56
Acknowledgments 56
References 56

Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services 58
Abstract 59
Introduction 59
Organization Requirements and Motivation 60
Related Work 61
Cloud Risk Management Process and Framework 62
Risk Management Process 62

Risk Control Matrix 64
Risk Management Framework 65
Discussion 67
Conclusion 68
References 68

ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services 70
Abstract 71
Introduction 71
Organization Motivation and Requirements 72
Related Work 73
Cloud Information Security, Privacy, and Compliance Readiness Model 73
Information Security Model (Cubic Model) 73
Readiness Factors 74
Readiness Assessment 76
Feasibility Analysis 76
Readiness of the Migration Plan 76
ISPC Readiness Flowchart 77
Discussion 78
Conclusion 78
References 80

SecSDLC: A Practical Life Cycle Approach for Cloud based Information Security 81
Abstract 82
Introduction 82
Related Work 83
SecSDLC Methodology 84
The Cloud Security System Development Life Cycle 84
Discussion 91
Conclusion 92
References 92

EVS: A Cloud Services Information Security and Privacy Eligibility and Verification System 95
Abstract 96
Introduction 96
Customer Motivation and Requirements 97
Related Work 97
Eligibility Verification System (EVS) Overview 97
The Cloud Security System Development Life Cycle 98
Conclusion 103
References 103

Secure Cloud Migration to a Compliant Cloud: A Case Study 104
Abstract 105
Introduction 105

Related Work 106
Case Study 106
Readiness Assessment and Decision Making Methodology 108
Conclusion 119
References 119

Conclusion and Future Research Directions 121
Summary 121
Future Research Directions 122

Bibliography 125

List of Abbreviations

(ISC)²	International Information Systems Security Certification Consortium
3PCAO	Third Party Assessment Organization
ACCA	Asia Cloud Computing Association
AIC	Administrator Interface Console
AIMS	Asset Inventory and Monitoring System
API	Application Programming Interface
CA	Cooperation Agent
CA	Control Audit
CAC	Compliance and Audit Checking
CCC	Cloud Customer Console
CCIPS	Cooperative Cloud Intrusion Prevention System
CCM	Cloud Control Matrix
CD	Customer Database
CIA	Confidentiality, Integrity, and Availability
CIF	Cloud Industry Forum
CM	Change Management
CME	Compliance Monitoring Engine
COBIT	Control Objectives for Information and Related Technology
CPO	Chief Privacy Officer
CRI	Cloud Readiness Index
CSA	Cloud Security Alliance
CSO	Chief Security Officer
CSR	Consultancy Service Request
DCA	Data Collector Agent
DDoS	Distributed Denial of Service
DIA	Data Inspection and Analysis
DIDS	Distributed Intrusion Detection System
DIPS	Distributed Intrusion Prevention System
DNS	Domain Name Service
DoS	Denial of Service
DPS	Department of Payment Systems
DSR	Design Science Research
EC	Eligibility Check
ENISA	European Network and Information Security Agency
ER	Event Response
ESR	Eligibility Service Request
EVS	Eligibility and Verification System

FedRAMP	Federal Risk Authorization Management Program
FISMA	Federal Information Security Management Act
GRC	Governance, Risk, and Compliance
HA	High Availability
HIPAA	Health Insurance Portability and Accountability Act
HP	High Performance
HRP	Historical Records and Performance
IA	Integration Agent
IaaS	Infrastructure as a Service
IDC	International Data Corporation
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSec	IP Security
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISPC	Information Security, Privacy, and Compliance
IT	Information Technology
KA	Keep-Alive
LD	Log Database
LS	Linkage Service
LTDB	Local Threat Database
NERC-CIP	North American Electricity Reliability Corporation-Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
OMV	Objectives, Mission, and Vision
OTR	Online Threat Repository
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry-Data Security Standards
POS	Point of Sale
PPTP	Point to Point Tunnelling Protocol
QoS	Quality of Service
RCCS	Risk Control and Compliance System
RMS	Risk Management System
SaaS	Software as a Service
SAM	System Agent Manager
SCM	Security Control Matrix
SDLC	System Development Life Cycle
SecSDLC	Security System Development Life Cycle
SecSLA	Secure Service Level Agreement
SEM	System Event Management

SESaaS	Security as a Service
SI	Statistical Information
SIEM	Security Information Event Management
SLA	Service Level Agreement
SNM	Security and Network Management
SOA	Service Oriented Architecture
SOC	Security Operations Center
SOCaaS	Security Operations Center as a Service
STS	Socio-Technical System
TCP	Trusted Computing Platform
TDA	Threat Detection Agent
UI	User Interface
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WEF	World Economic Forum

List of Tables

The Results of a 2013 (ISC)² Survey of the Global Information Security Workforce on the Skills Required in Dealing with Cloud Computing 26
The Trust Model Attributes 30
Cloud Industry Forum Cloud Adoption and Trends Survey 2011 60
Important Threats to Information Security and Data Privacy 63
Measurement Levels for Cloud ISPC Readiness 75
The Cloud Security System Development Life Cycle (SecSDLC) Methodology Tools and Measures 90
Design Science Research (DSR) Guidelines 98
Cloud Deployment and Service Model 106
Summary - Information Security, Privacy, and Compliance Control Family 113
Measurement Levels for Cloud ISPC Readiness 114
Current ISPC Readiness 114
Desired ISPC Readiness 114
Department of Payment Systems (DPS) Migration Readiness 116

List of Figures

Cloud Computing Service Models 17
IDC Survey Results Regarding Issues in Cloud Computing 17
The Cooperative Cloud Intrusion and Prevention System (CCIPS) Architecture 20
The Cooperative Cloud Intrusion and Prevention System (CCIPS) - Distributed Across the Country 21
The IaaS and Application CCIPS Framework 29
The STS Based Trust Model 30
The Proposed Trusted CCIPS Model 32
The SOCaaS Operational Process Timeline 38
The Cloud Computer Security Model 39
The Security Operations Center as a Service (SOCaaS) System Architecture 44
The Activity Theory System Model 51
The Security and Privacy Control Request Negotiation Workflow 53
The SecSLA System Framework 55
The Risk Control Strategy Matrix 64
The Cloud Risk Management System 65
The 2011 World Economic Forum Advanced Cloud Computing Report 72
The Information Security, Privacy, and Compliance (ISPC) Cubic Model 74
The SecSDLC Methodology 91
The Eligibility and Verification System (EVS) Architecture 99
The EVS Linkage Process 100

Acknowledgments

"In the name of Allah, Most Gracious, Most Merciful"

Alhamdulillah, all praises to Allah for the strengths and his blessing in completing this dissertation.

I would like to express my special appreciation to my advisor, Dr. T. Aaron Gulliver, for his supervision and constant support. His tremendous help of constructive comments and suggestions throughout the dissertation work have contributed to the success of this research. I would also like to thank him for encouraging my research and for allowing me to grow as a research scientist

My acknowledgement is also due to Dr. Daler N. Rakhmatov and Dr. Sudhakar Ganti for serving as my committee members and their cooperation, comments and constructive criticism. I would also like to thank you for your brilliant comments and suggestions and for making my research enjoyable.

Dedication

I would like to dedicate this work to my wonderful parents, who have loved me unconditionally and whose good examples and their emphasis on the importance of education have taught me to work hard and smart for the things I aspire to achieve.

This work is also dedicated for my beautiful and lovely wife, *Amal*, who has been a source of endless support and encouragement, I am truly thankful for having you.

To my greatest accomplishment, my son *Abdullaziz*, who has grown into a wonderful two years old in spite of his father spending so much time away from him working on his project and this dissertation, I dedicate this doctoral degree to you as I know you will take advantage of our hard work and put your keen intellect to full use to become highly successful at whatever you choose to do.

Chapter 1

Introduction

Background

Cloud Computing refers to a paradigm of a network that distributes processing power, applications, and large systems among many computing resources over the Internet [1]. Its emergence promises to streamline the on-demand delivery of hardware, software, and data as a rented service, achieving economies of scale for faster information technology (IT) development, deployment, and operation. Cloud computing concept dates back as early as 1961 when Professor John McCarthy envisioned a time-sharing technology that might lead to a future with application and computing power that might be sold through a utility based business model [2]. His idea became popular in the late 1960s but soon the idea faded away due to the lack of a sustainable computing model [3].

The emergence of cloud computing is based on utility computing which is defined as the provision of computational processes and storage resources as metered services, similar to public utility services such as electricity. The concept is growing in popularity as many IT departments want to access and manage their services on demand and from anywhere. Further, the term ‘cloud’ and ‘computing’ cause confusion, but become much more understandable when one thinks how a modern IT environment works, scales, and dynamically increases or decreases its infrastructure without the need to invest money in acquiring new infrastructure, training, or new software licensing [3].

In late 2007, cloud computing services became a hot topic in IT industry due to its flexibility to offer a great degree of flexible and dynamic IT infrastructure deployment. The advancements of computational power, quality of service, and the speed of Internet allows users to move out their data and applications to the remote “Cloud” [4]. Nowadays, cloud computing becomes a solution option for those seeking to build a complex IT environment. When IT professionals have to manage various network and system installations, configuration, and updates, outsourcing these tasks to the cloud is a smart solution to handle complexities within IT operations [5].

Cloud services benefits attract many organizations wanting to avoid capital expenditures on running IT platform, hardware, software, and applications. The cloud enables these organizations to pay only for what they use. Cloud providers usually bill their customers on their consumption of the services rented or subscribed, usually with little to no upfront cost. Cloud services characteristics provide elastic capacity for customers wanting to scale up or down their rented services in response to their business change requirements. Further, they offer tools for rapid adoption of new application development allowing customers the ability to test their prototype application, optimize, and measure it performance prior to production deployment [6].

There are a number of enabling technologies behind cloud offerings. The main ones are:

- Virtualization and automation technology that allows partitioning the hardware to accommodate multiple operating systems, storage, and CPU resources to be shared among multiple tenants without affecting the anticipated end performance. This technology is fundamental architectural principle for cloud services. It refers to the abstraction of computing resources i.e., virtual machine (VM), a software that allows multiple operating systems to execute programs and applications using one dedicated hardware resource. Cloud service provider replies on its VM, such as VMware [7] and Xen [8], to render flexible and scalable hardware, platform, and software resources.
- Cloud storage technology offers scalable and distributed storage capacity for customers to lease. Customers can upload, merge, manage, and expand their storage on demand. Examples such as Google Drive [9] and Amazon S3 [10] for file management.
- Service oriented architecture (SOA) is embedded into cloud services in order to simplify Internet. The SOA supports various platforms to enable data collaboration and cloud activity coordination. The SOA is designed based on open standards making communication between cloud customers and their services simple and less dependent on technology vendors or any proprietary communication protocols [11].

National Institute of Standards and Technology (NIST) defines cloud computing as: *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models"* [12]. Cloud computing defined by NIST have three service models, Infrastructure as a Services (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS enables cloud customers to buy fully outsourced infrastructure that includes servicers, software, and network equipment. PaaS allows customers to rent virtualized servers and multiple operating systems in order to run their production and test applications. SaaS provides application or software as a service on demand accessible from a browser such as web-based email or program interface [12], [13].

The above cloud service models have four options of deployment. A Public deployment where cloud infrastructure is provisioned for general public where no security measures are required. Public cloud is considered the lowest cost among cloud deployment models. A community deployment enables sharing the cost and cloud resources among fewer customers. The community cloud offers a higher level of security and privacy compared to the public cloud. The third deployment is private clouds where customers exclusively rent, build, and manage their IT resources. While private cloud reduces the security and privacy risks to the minimal and offers the highest degree of control [12], [14], it relatively considered a high cost deployment. Subsequently, an organization that wants to migrate to the cloud services yet retains all the benefits of public cost effectiveness and the security and privacy of private cloud choose a hybrid, the fourth deployment of cloud service, of cloud deployment models that suits their requirements [14]. Figure 1 shows the different deployment methods along with cloud service models.

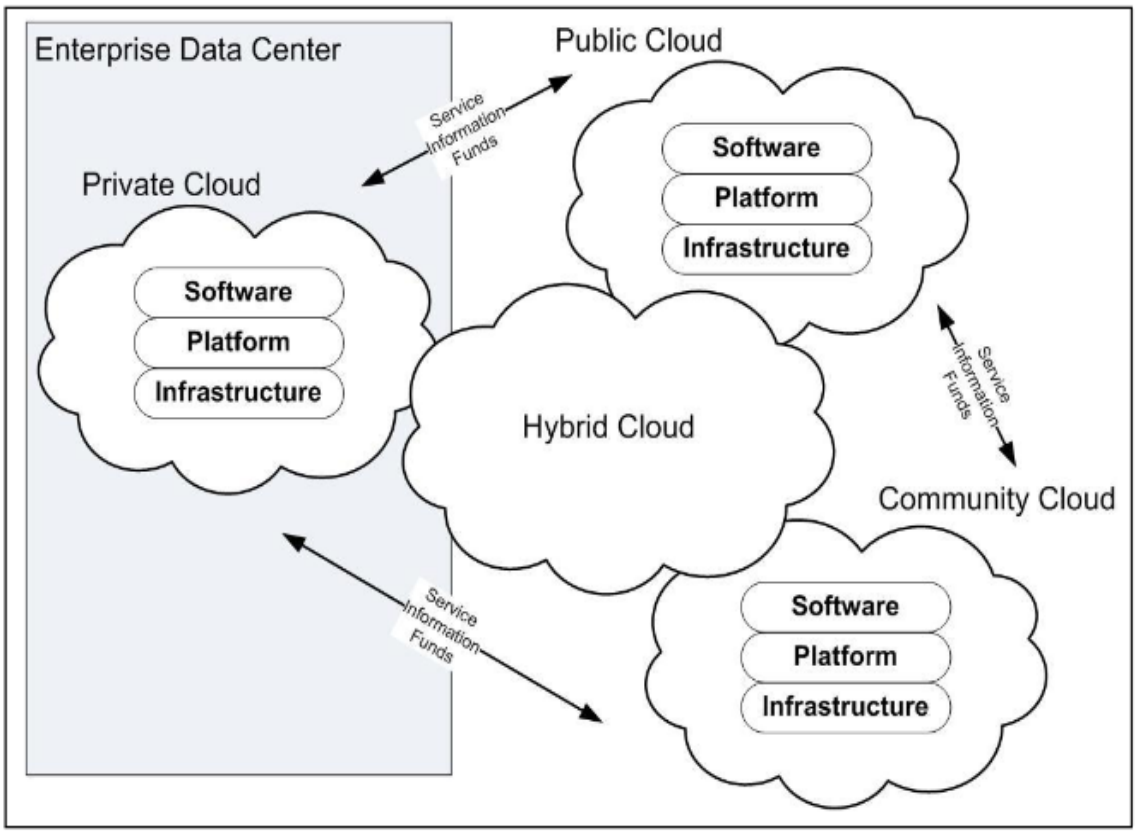


Figure 1 Cloud service and deployment models.

Cloud services become the key computing platform for sharing resources that include infrastructure, software, and applications. Moving organization's data into the cloud offers great opportunities to avoid complexities from direct involvement in building, operating, and managing IT resources. While cloud services provide an ample amount of storage space with customizable computing resources, they however eliminate or minimize the control over these acquired services. In other words, cloud customers are at the mercy of their cloud service providers for the confidentiality, integrity, and availability (CIA) of their data [15-17]. Although outsourcing organization's data into the cloud is cost-effective and less complex, it lacks strong information assurance in terms of CIA aspects, which may impede the adoption of cloud services especially by highly classified organizations [18-20].

Research Motivations

The traditional IT infrastructure issues still exist and have similar patterns to threats affecting cloud services. When organizations offload their IT infrastructure including their applications and data to the cloud, their existing traditional security measures are no longer suitable to protect their resource. Therefore, cloud customers are still reluctant to deploy their business and IT resources to the cloud. In addition, these security issues slow the acceptance to migrate sensitive and sometimes public data to the cloud [21].

The cloud multi-tenancy architecture brings tremendous impact on information security due to its dynamic scalability, service abstraction, and location independence characteristic in cloud service models. In addition to these characteristics, conflict of interest may appear when data outsourced to multiple service providers introducing the unforeseen complexities in meeting unified security measures. The virtualization concept introduces the openness of resource sharing by multi-tenant. This may allow threats of unauthorized access to other customer's data [22]. The Cloud Security Alliance (CSA), a non-profit organization striving to provide security standards and guidelines to cloud services, encourages cloud service providers to participate into forming the best practices to address the security, privacy, compliance, and contractual issues many cloud customers are facing [23]. The CSA has identified thirteen areas of concern to meet the minimum requirements for information assurance [24].

When organizations migrate to the cloud, they know neither the exact location of their data storage or processing nor if other customer data, collectively, stored with theirs. Cloud services are Internet-based service delivery where the infrastructure, platform, application, and software are made available and accessed anywhere at any time. The data classifications found in the cloud range from public resource, that implies minimal security concerns, to highly classified data such as social security number, corporate financial records, trade-secrets, or medical records. Many organizations are well aware of the ability to secure their online communications by using secure socket layer (SSL) encryption along with the use of strong authentication measures. However, offloading their data, especially sensitive data, to the cloud requires careful consideration of

security, and privacy, and compliance measures implemented by cloud providers. With proper adoption of a comprehensive information security system, the Internet service delivery which is the backbone of cloud services, can provide the flexibility and security required by organizations of all sizes. The motivation of this research can be grouped around resolving cloud customers concerns which are:

CIA Triad: with all its benefits, cloud computing brings with it concerns about confidentiality, integrity, and availability (CIA) of information extant on the cloud as a result of its multi-tenancy structure, lack of detailed information security program, and geographical dispersion. Such concerns:

- Data leakage and unauthorized access of data,
- Inappropriate information handling by cloud providers to protect sensitive data,
- Release of critical data to law enforcement or third party without the customer's consent,
- Lack of measures to meet compliance and regulatory requirements,,
- Lack of processes and measures in place to manage the risk of service disruption, such as backup Internet network links, redundant storage and effective data backup and restore mechanisms. As a result, customers are unable to access their service, availability concern, for an extended period of time.
- Cloud providers implement minimal measures to ensure data integrity (e.g., detecting alterations to sensitive data by cryptographic mechanisms such as message authentication or digital signatures),
- Cloud providers implement minimal or weak measures to ensure confidentiality (e.g., encryption of sensitive data 'in transit' and 'at rest' authorization mechanism and strong authentication). Confidentiality from a contractual point of view is minimal or weak, such as confidentiality and non-disclosure agreements or clauses such as policies and procedures binding upon the cloud service providers and any of its employees who may be able to access the customer's sensitive data and assurance that only authorized persons can have access to data,

- Insecure applications, such as cloud application programming interface (API), implemented by service provider allows hackers to customer's sensitive data and login credentials.
- The security systems instituted by cloud provider are inefficient and do not meet customer's expectations for in-depth CIA requirements.

Costs: the cloud proposition allows organizations and start-up companies to greatly reduce cost associated with starting up their business and IT infrastructure. Cloud computing services offers IT infrastructure and platform that are already in place minimizing time and other resources need to build a data center [25].

Trust: The information security program adopted by cloud providers should be designed to protect cloud systems from malicious threats and intrusions. They must ensure that their security program is trusted to act in specific and predictable manner as intended and promised in their contractual agreement i.e., service level agreement. There are concerns when it comes to trusting the cloud provider's security mechanisms, its effectiveness and transparency. Such concerns are [26]:

- The ability of cloud provider's security program to protect data in use and its boundaries when one virtual machine is responsible to manage multiple cloud customers,
- The location of data while in storage, process, or in transit,
- Lack of customer's control over data,
- Lack of detailed documentation in regards to information security policies, compliance mandates, disaster recovery, and incident response plan, and
- Lack of transparent processes and procedures for addressing the above concerns.

Legal and regulatory constraints: Organizations wanting to migrate to the cloud are facing challenging task when it comes to understanding the regal boundaries they have to abide by. The problem is even more complex when considering cloud services due to its international distribution of processing and storing data subject to regulatory constraints [27]. For instance, an organization might be subject to comply with regulations for

privacy needs to ensure the necessary measures are employed by its potential cloud provider to meet the minimal requirements of data privacy. In December 2014, CSA released a privacy level agreement for Europe [28] in an effort to be accepted by many cloud service providers. The CSA privacy agreement document contains a set of eleven questions that help cloud providers better shape privacy controls and provide transparent answers to potential customers. Questions such as [29]:

- Identify the procedures used to inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or sub processors with the cloud customers retaining at all times the possibility to object to such changes or to terminate the contract.
- Identify the subcontractors and sub processors that participate in the data processing, the chain of accountability and approach used to ensure that data protection requirements are fulfilled.
- Specify the location(s) of all data centers where personal data may be processed, and in particular, where and how they may be stored, mirrored, backed-up, and recovered.
- Indicate whether data is to be transferred, backed-up and/or recovered across borders, in the regular course of operations or in an emergency. If such transfer is restricted under applicable laws, identify the legal ground for the transfer (including onward transfers through several layers of subcontractors): e.g., European Commission adequacy decision, model contracts, Safe Harbor, Binding Corporate Rules (BCR).
- Specify the technical, physical and organizational measures in place to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized use, modification, disclosure or access and against all other unlawful forms of processing.

Research Methodology

The implementation of a suitable methodology, which adequately encompasses the specific research objectives set out in this research, was essential. The process of

progressing from the initial problem formulation to the final integrated proactive detection and prevention and secure service level agreement frameworks involved several iterations prior to achieving the specified objectives and development of these frameworks. The implementation of the developed research methodology was formulated around nine scientific research papers. Each of these studies focused on a specific set of cloud concerns found in industry and research with the respective scientific outcomes. The multivariate analysis method was beneficial for exploring and understanding relationships between different cloud customers, information security policies, controls, and regulatory mandates in order to identify missing patterns in current cloud security measures. The human factors such as awareness of cloud issues, training, and management decisions, were important in research methodology to formulate correlations utilized in framework design and development.

Each paper incorporates relevant information security theories and best practice models in the design and development process. Paper 1, for example, adopts the design principles based on the National Institute of Standards and Technology (NIST) risk management guidelines and recommendations [30]. Paper 2 utilizes information security theory such as Socio-Technical System (STS) theory, which is used to enable knowledge sharing and allow cloud customers and service providers to collaborate in designing and evaluating systems performance. Paper 3 employs information security management model [31] and cloud security model [32] that is based on deterrence theory adopted from the discipline of criminology [33] to develop deterrents, detection, and prevention framework for cloud security operations center. The taxonomy of cloud security control matrix, listed in Paper 4, is based on cloud security alliance (CSA) recommendations [34]. Paper 4 combines the application of activity theory introduced by Engestrom [35], which provides a basis for determining security controls and actions for noncompliance and violations, with cloud security control matrix to devise secure service level agreement framework.

New frameworks and methodologies are proposed in Papers 5, 6, and 7 for the construction, deployment, measurement, and delivery of an effective cloud based information security program. These are based on mixture of best practice and guidelines

developed by the cloud security alliance (CSA) [12] in conjunction with a cloud controls matrix (CCM) [13] to manage cloud security risks and threats. The suggested cubic security control model is also aligned with industry accepted security standards and follows guidelines such as NIST SP800-53, COBIT, ENISA IAF, HIPAA, ISO 27001/27002, NERC CIP, PCI DSS, and FedRAMP [13]. The maturity assessment of cloud service provider and readiness evaluation for cloud customers for migration were introduced in Paper 6 i.e., readiness model, and were created in light of systems security engineering capability maturity model (SSE-CMM) [12]. Further efforts were to extend the previous work to help addressing the missing and/or weak cloud information security program via six-phase systematic approach i.e., the security system development life cycle in Paper 7.

Cloud customers are concerned with the transparency, compliance, and trustworthiness of CPs. The system presented in Paper 8 is based on design science research (DSR) methodology [36], [37] that provides specific set of concepts and principles to develop IT solutions. The eligibility and verification system solution in Paper 8 promotes transparency and trustworthiness of cloud services by monitoring cloud customer security control compliance using trusted third party. The last paper in this dissertation presents a case study in an effort to address real life challenge using some of our new frameworks and models. The case study design and methodology are based on Yin [38] and Baxter and Jack [39], in addition to the approach used in our conceptual frameworks. The case study validates our previous work around Yin, Baxter and Jack guidelines for exploring possible solutions for the help the migration decision making using a variety of sources. Additionally, Yin suggested a case study design to be used when research questions attempt to address ‘when’ and ‘why questions. The detailed description of the linkage of these scientific papers and their outcomes in relation to the developed frameworks are provided next.

Linkage of Scientific Papers

Satisfactory performance of cloud services, in particular cloud information security, privacy, and compliance systems, depends mainly on the predictive and proactive ability to detect and prevent threats and risks affecting cloud community i.e., cloud customers, providers, and other stakeholders. Consequently, one of the most important issues regarding the appropriate use of cloud services is the use of proper assessment to the cloud services and their characteristics which play a vital role in the identifying risks, performance gaps in information security policies, and countermeasures. However, current cloud security methods, policies, and measures have only limited set of controls that hinder many organizations wanting to migrate their IT infrastructure to the cloud. Although, cloud service providers methods may be adequate for some organizations with low level of data sensitivity, they do not necessarily indicate their appropriateness for those with higher level of data classifications.

The concept of intrusion detection and prevention (ability to proactively detect, remove, and adequately respond to threats and risks) is described in details through Papers 1, 2, and 3. Paper 1 *(CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services)* outlines a framework for detecting and preventing known and zero-day threats targeting cloud computing networks. The CCIPS framework formed the basis for implementing enhanced threat detection and prevention via behavioral and anomaly data analysis. Paper 2 *(A Trusted CCIPS Framework)* scales the work of CCIPS to promote security and privacy in cloud environment. The trusted CCIPS model details and justifies the multi-layer approach to enhance the performance and efficiency of detecting and preventing cloud threats.

Both Papers 1 and 2 investigate the ability for cloud providers to proactively detect and prevent cloud services from known and unknown incidents (newly born suspicious activities that may cause harm). However, although these papers use various layers of defense techniques to assess cloud threats, a detailed description of incident management methods (event collection, handling, analysis, response, and forensics) were not the main focus of these studies. Therefore, Paper 3 *(SOCaaS: Security Operations Center as a*

Service for Cloud Computing Environments) provides a more detailed discussion on implementing unified yet comprehensive security operations center for assessing cloud based services with major focus on the event analysis. The SOCaaS enables cloud customers to have real-time monitoring and security management for suspicious events that may cause harm to their cloud services and information. The combined outcomes from Papers 1, 2, and 3 provided a more scientific basis for assessing the ability of cloud service providers to, proactively, address concerns related to customer's information security.

Although cloud service providers have significant role in addressing information security, privacy, and compliance, inadequate service level agreements between CPs and their potential customers have led to missing gaps found later in customers' information security, privacy, and compliance requirements. Paper 4 *(SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services)* highlights the need for better mechanisms for identifying those gaps in early stages of the agreement. This helps both customers and service providers ensuring transparent and adequate security, privacy, and compliance requirements are addressed, enforced, and continuously monitored. The paper analysis on the collected cloud information security controls highlighted the need to devise a cloud based security control matrix addressing the control provisioning gaps found in current providers' service level agreements. Additionally, it was also evident that some factors, such as control enforcement and monitoring, play important roles which either decrease or increase the compliance extent of the acquired service level agreement and security program. Both Paper 3 and 4 describe the need for having a trusted and competent third party entity to foster the suggested approaches in an effort to leverage transparency and trust in cloud community.

The low cost model, flexibility and accessibility characteristics of the cloud services have resulted in a rushed decision to adopt the cloud. Without the proper attention to cloud services information security and privacy issues, the adoption will most likely lead to critical business impact due to higher likelihood of security risk occurrence. This research contributes to reducing this uncertainty by utilizing the development of integrated risk

management framework described in Paper 5 *(An Effective Risk Management Framework for Cloud Computing Services)* which seek to implement systematic approach to conducting risk identification, assessment, and control that fits the cloud environment. Meanwhile, the uncertainty of risk occurrence can be further reduced using the readiness model in Paper 6 *(An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services)* allowing for the early identification and of those at risk areas prior the migration plan. Even after the migration, it was observed that the tools and guidelines provided in Paper 6 enable organizations to evaluate their readiness to effectively detect and counter cloud threats and compliance violations.

Cloud applications and services undergo constant changes and feature additions, and hence an effective information security system is needed to appropriately address any issues those constant changes and additions might bring. The goal of Paper 7 *(A Practical Life Cycle Approach for Cloud based Information Security)* aims to provide a holistic methodology that helps to design and implement an effective information security system that can quickly adopt to such changes. The discussion through all the previous seven papers, agree on the inherent difficulty in identifying ISPC compliant cloud technology which was observed through the literature and the case studies as a necessity to be able to accurately identify and categorise the various source of compliant cloud providers. The use of a trusted system for tracking and monitoring ISPC controls, namely eligibility and verification system was introduced in Paper 8 (Cloud Services Information Security and Privacy Eligibility and Verification System) to help resolving the identification of compliant cloud service providers.

The real implementation of the technical aspects of the previous 8 papers faces multiple challenges such as the lack of applicable cloud management platforms and simulators. Subsequently, a case study of some of these frameworks and models is presented in Chapter 10 to address the real-life challenges faced by a financial agency in Saudi Arabia. This study presents a possible implementation of the work discussed in the previous papers, to help the decision making process faced by the Saudi financial agency for migrating their IT services to the cloud.

Together these models and frameworks suggest that the threats and risks associated with cloud services are continuously changing and importantly, increasing in complexity and sophistication, contribute to make stronger cloud based information security, privacy, and compliance technological frameworks. The results presented in this dissertation have significantly contribute to the best practices in ensuring information security controls are addressed, monitoring, enforced, and compliant with relevant regulations.

Chapter 2

CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services

As published in *International Journal of Latest Trends in Computing*,
December 2013

This article appeared in Vol. 4, Issue. 4, published by *International Journal of Latest trends, Copyrighted to © ExcelingTech Publisher, UK*. The attached copy is furnished to the author for internal non-commercial research and education use, including for instructions of the authors institution and sharing with colleagues.
Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.
In most cases authors are permitted to post their version of the article to their personal websites or institutional repository. http://ojs.excelingtech.co.uk/

CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services

Fahad F. Alruwaili[12] and T. Aaron Gulliver[3]

Department of Electrical and Computer Engineering
University of Victoria, PO Box 3055, STN CSC
Victoria, BC V8W 3P6, Canada

[1]fruwaili@uvic.ca
[3]agullive@ece.uvic.ca

***Abstract*— With the recent emergence and rapid advancement of cloud computing infrastructure and services, outsourcing Information Technology (IT) and digital services to Cloud Providers (CPs) has become attractive. This will allow for a reduction in IT resources (hardware, software, services, support, and staffing), and provide flexibility and agility in resource allocation, data and resource delivery, fault-tolerance, and scalability. However, the majority of cloud service providers tailor their services to address functionality (such as availability, speed, and utilization) and design requirements (such as integration), rather than protection against cyber-attacks and associated security issues. This paper considers the detection and prevention of security attacks against cloud computing systems. A proactive Cooperative Cloud Intrusion Prevention System (CCIPS) framework is proposed to detect and prevent known and zero-day threats targeting cloud computing networks. This framework provides enhanced threat detection and prevention via behavioral and anomaly data analysis. A multi-layer approach to security is employed to provide a cooperative model cloud which has both high performance and high availability.**

***Keywords*—** Availability, Virtualization, Intrusion Detection, Intrusion Prevention, Attacks, Threats, Cloud Computing.

[2]The research of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia

1. Introduction

The concept of cloud computing was first conceived over 40 years ago as the virtualization of resources to allow users access to significant computing power and resources [1]. The term virtual comes from the telecommunications concept of a virtual private network (VPN). VPNs were developed to provide secure data and voice channels. Foster et at. [2] define cloud computing as, "a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet."

Cloud computing services are delivered on demand and pay-per-use via internet web browser protocols (HTTP and HTTPS). They are configured dynamically for service delivery based on contractual agreements between cloud service provider and users (tenants). Corporations, governments and academic institutions are actively considering the adoption of cloud computing services to lower costs, improve performance, increase storage capacity, provide interoperability, and reduce power consumption (green IT) [2].

Cloud computing can provide numerous services through web-enabled applications [3]. These can be classified into three main cloud service models [4], as shown in Figure 1. They are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). With IaaS, cloud service providers can deliver processing, storage, and network resources to host user systems (e.g., Amazon EC2). The PaaS cloud service model provides users with the ability to deploy, control, manage, and customize their applications. However, they cannot control or manage the underlying IaaS resources (e.g., Microsoft Azure) that operate and support the

Copyright © ExcelingTech, Pub, UK (http://excelingtech.co.uk/)

applications. SaaS is an upper cloud service model where users have access to applications owned and managed by the cloud providers (e.g., Gmail).

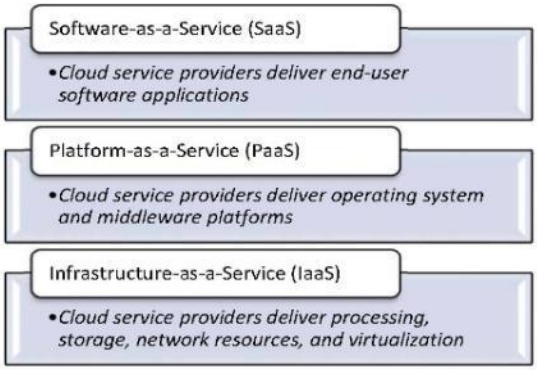


Figure 1 The cloud computing service models.

Although many organizations are considering cloud computing due to its many advantages, this outsourcing makes it difficult to maintain data integrity and privacy, support data and service availability, and demonstrate compliance [5]. Therefore, providing a standardized security framework is an important and challenging issue in cloud computing. Both cloud customers and service providers face common concerns that must be addressed to ensure successful cloud service adoption and delivery.

In 2009, the International Data Corporation (IDC), a leading market research and advisory organization, conducted a survey of more than 260 IT executives and managers to gather their opinions and concerns regarding cloud computing [6]. Their report indicates that security is the top priority, as shown in Figure 2. The concern is that critical IT resources and information in cloud systems might be vulnerable to cyber-attacks or unauthorized access [7]. The primary security concerns with cloud environments pertain to security, availability and performance. Many attacks are designed to block users from accessing services and providers from delivering services, i.e., denial of service. Service providers may face significant penalties due to their inability to deliver services to customers in accordance with regulatory requirements and Service Level Agreements (SLA) [8].

Figure 2 IDC survey results regarding issues in cloud computing (3Q 2009) [6].

This paper proposes an intrusion prevention framework which leverages current intrusion detection solutions. This framework is designed to satisfy specific security requirements within a distributed information system. It integrates the detection and prevention of known and new threats via the detection of traffic abnormalities and process monitoring. The Cooperative Cloud Intrusion Prevention System (CCIPS) framework protects the IaaS cloud computing service model as it is the cloud service foundation layer. Thus other cloud computing service models are not considered here.

The framework is based on current approaches proposed in the literature and employed in industry. We focus on the implementation of intrusion detection and prevention mechanisms in a cloud environment. The design is based on the National Institute of Standards and Technology (NIST) risk management guidelines and recommendations [9].

2. Background and Related Work

In this section, we discuss current threats to cloud computing services. Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) are considered. While there are many potential threats to cloud services, the focus here is on the cloud IaaS service model and the corresponding framework.

A multi-tenancy architecture in a cloud computing environment allows customers to share a single infrastructure and store their data in one database system. Therefore Virtual Machine (VM) hopping where one customer gains access to the VM of another

is a threat [10]. Another threat is the disruption of cloud services due to a Distributed Denial of Service (DDoS) attack. These attacks produce a massive number of fake connection requests to a cloud service. If the targeted service is unable to respond to these requests, the result is a loss of service. Due to the nature of a cloud computing environment, this can affect a large number of users. Countermeasures include increasing the number of resources and employing an effective Intrusion Prevention System (IPS) [11].

Attacks attempting to gain unauthorized access and control over the hypervisor engine (the operating system responsible for managing multiple operating systems), or the virtual machine monitor (VMM), are considered to be the most serious threats to cloud computing services. This is particularly true for the IaaS cloud service model [12].

2.1. Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is designed to actively monitor and analyse network traffic. It performs predefined actions in response to suspicious behaviour. Yassin et al. [13] proposed a Cloud-Based Intrusion Detection System (CBIDS) to detect and notify users of suspicious content within the cloud environment. This improves on legacy IDS systems which were not designed to be deployed in a cloud infrastructure.

Kourai and Chiba [14] proposed a distributed monitoring system called HyperSpector for virtually distributed computing systems. It isolates the IDS from the virtual server it monitors in order to increase server security and protect the IDS system from active attacks. HyperSpector was introduced to only monitor VM and IDS systems, so preventative measures were not considered.

In [12], Laniepce et al. proposed an approach to IDS in cloud environments which exploits virtualization to monitor all virtual services and the resources dedicated to VMs. It is a hypervisor-based Intrusion Detection and Prevention System (IDPS) and was the first to provide IDS deployment in the IaaS cloud computing model. They suggest that the hypervisor-based IDPS be placed within a VM to enable the detection and prevention of VM attacks.

Zargar et at. [17] proposed a Distributed, Cooperative, Data-driven Intrusion Detection and Prevention (DCDIDP) framework. Cloud service providers that employ this framework benefit from cooperative intrusion detection, which provides fast response. The DCDIDP framework uses three cooperative databases for threat detection and prevention, the intrusion assessment information base (IAJB), the policy and rule base (PRB), and the audit logs database.

2.2. Intrusion Prevention System (IPS)

Intrusion Prevention Systems (IPSs) have additional security features compared to an IDS. A combination of features is employed to provide real-time response to attacks and threats [15]. An IPS requires minimal user or system administrator interaction.

Jin et al. [16] proposed a system called VMFence for real-time monitoring of data flow and file integrity in a cloud computing environment. This system features high availability and high performance (i.e., fast response). VMFence was designed to detect intrusions in data packets and user files.

3. Design Objectives

In a typical data centre, attacks such as denial of service are mitigated by implementing front-end protection using an IDS and/or IPS. These systems detect patterns in the traffic by analysing packets based on an up-to-date signature file. If a flag is triggered based on this analysis, the IPS will request that a network protection agent take action as a countermeasure to the corresponding attack. Since an IPS is itself subject to failure due to an attack such as DoS, a fault tolerant system is desirable. Thus a Distributed Intrusion Prevention System (DIPS) is developed to avoid a single point of failure [13].

Existing IDS and DIDS designs have several deficiencies which should be addressed. These are outlined below.

- IDS systems are passive with a limited set of actions. Usually, these actions are just email alerts and/or email reports.
- IDS systems detect threats such as DoS attacks using only predefined signatures and patterns. Thus zero day (unknown) attacks will likely go undetected.

The Cooperative Cloud Intrusion Prevention Framework

Based on these issues, a framework that prevents cloud services from both known and zero-day (unknown) attacks is developed in this paper. This Distributed Cooperative Cloud Intrusion Prevention System (DCCIPS) provides robust prevention mechanisms, accurate alerts, fast reaction to known attacks, and proactive actions to counter zero-day attacks. This is done via detailed examination of traffic behaviour. The framework is based on the National Institute of Standards and Technology (NIST) risk management guidelines [9] to address threats to the IaaS service model in cloud computing. Based on an analysis of current intrusion detection and intrusion prevention systems, an improvement to previous IDS and IPS solutions is proposed. The proposed Cooperative Cloud Intrusion Prevention System (CCIPS) framework is presented in the next section.

4. The Cooperative Cloud Intrusion Prevention Framework

The goal of the proposed Cooperative Cloud Intrusion Prevention System (CCIPS) is to protect service providers and their clients against loss of services from known and unknown threats. It provides fast threat detection and accurate response through collaboration among distributed CCIPS systems. The threat database and system event logs are updated from multiple locations to provide improved threat detection accuracy. This will reduce the false negative detection rate (failing to identify threats), and the false positive detection rate (reporting normal or expected behaviour as anomalous or malicious).

The CCIPS is designed to proactively monitor up to the network layer (IP layer) in the cloud virtualization. Unlike existing intrusion detection systems, the proposed framework takes action by dropping and blocking internet connection(s) that can cause a denial of service. The source Internet Protocol (IP) address and other incident information are logged for further action. In addition, the CCIPS is designed to be cooperative locally where two systems are active for load-balancing and/or load sharing of CCIPS activities. The coordination of these activities is handled by a keep-alive agent. This enables high availability (HA) and high performance (HP) through inline (parallel) active backup CCIPSs.

There are two states of incoming traffic. The normal state indicates usual traffic behaviour (no threats). The suspicious state indicates anomalous traffic behaviour. There are two databases in the CCIPS model.

- The first database contains the signatures of all threats known to date.
- The second database is an anomaly database that contains patterns of abnormal network traffic behavior. It also contains normal state system logs to allow for the detection of abnormal behavior when a deviation from this state occurs. For this database to be effective, a cloud service provider must have accumulated sufficient information on normal behavior.

All incoming packets are analyzed by the CCIPS. If a packet is not determined to be legitimate based on the rule or signature database, it is considered suspicious so CCIPS flags this as an incident which could be an intrusion, DoS attack, or zero-day (unknown) attack. Upon further investigation, the connection is either dropped or added to the anomaly database as legitimate traffic. This process compares the packet against the log file over a predefined period (e.g., several days or weeks). If a connection with an unusual activity pattern is detected (e.g., an anomaly is detected by the CCIPS), cloud providers can take appropriate action to protect against service interruptions. This provides protection against threats with no signature (i.e., zero-day attacks).

Figure 3 presents the CCIPS architecture. Note that there can be multiple active CCIPS backups. The CCIPS system is designed to be highly available in order to provide reliable protection against cloud service interruptions. An agent with non-invasive keep-alive or hello-check messages is employed to sense the connections between CCIPS operating systems (i.e., master and active backup CCIPSs). This approach can be expanded to include additional inline active CCIPSs as backup systems to provide improved performance via redundancy.

The CCIPS architecture provides high availability and performance through a master and multiple active backup CCIPS, i.e., a cluster structure. With this approach, the CCIPS architecture can be distributed across the cloud provider enterprise as shown in Figure 4. Several cloud providers can collaborate on threat detection to provide faster response. Each CCIPS consists of eight modules as described below.

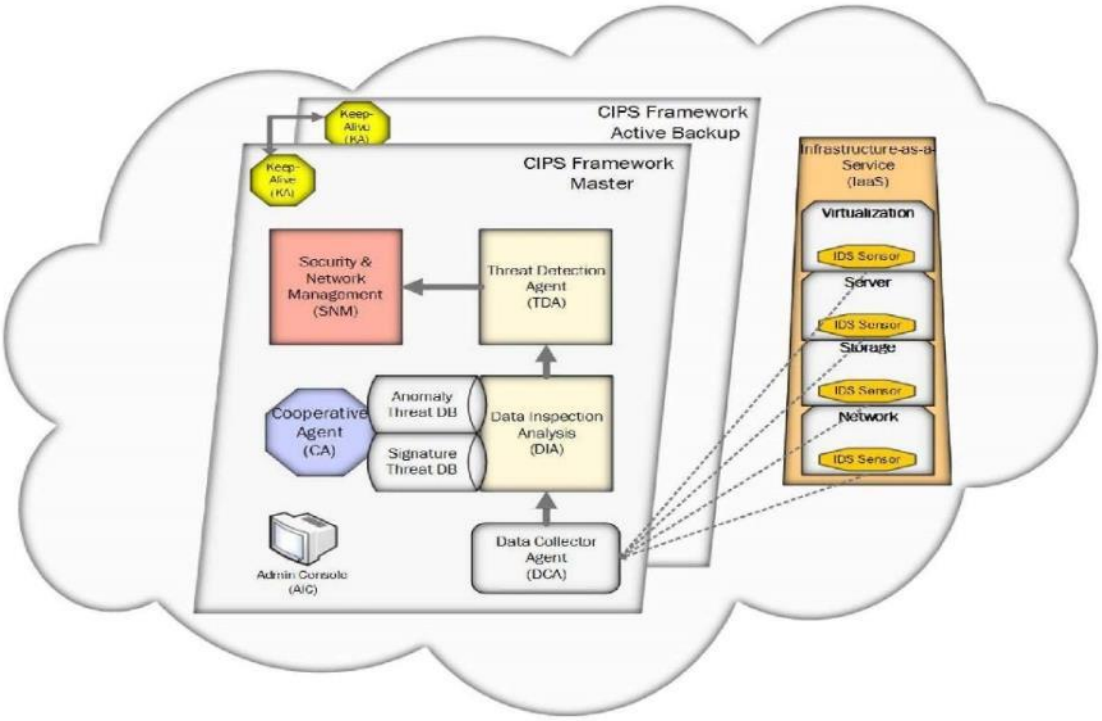


Figure 3 The Cooperative Cloud Intrusion and Prevention System (CCIPS) Architecture.

4.1. Threat Detection Agent (TDA)

At the core of the CCIPS are two monitoring modules.

The *Anomaly Detector* is responsible for detecting patterns of unusual or abusive behavior. It works inline with the anomaly database which contains patterns of behavior associated with known attacks. It also monitors the system operation.

The *Intrusion Detector* is responsible for monitoring traffic and detecting known threats. It works inline with the signature database which is always up-to-date.

4.2. Intrusion Detection Sensor (IDS)

This sensor is an integral part of every component of IaaS model. As shown in Figure 3, to aggregate activity logs, intrusion detection sensors are placed in:

the *Network layer* for monitoring incoming, outgoing, and local network activities;
the *Storage layer* for monitoring file integrity and unauthorized file access to provide file protection;
the *Server layer* for monitoring CPU usage, process activities, memory, and input/output (I/O) utilization; and
the *Virtualization layer* (*hypervisor*) for monitoring configuration files and all process instances and activities of VMs.

4.3. Data Collector Agent (DCA)

Based on predefined scheduling intervals, the DCA receives all packets from the deployed IDSs in the IaaS components. The aggregated data is then passed to the Data Inspection and Analysis (DIA) module for inspection and auditing. The DCA not only collects packets but also detects sensor failures so the CCIPS is reactive to internal failure of detection services.

4.4. Data Inspection and Analysis (DIA)

This module receives packets collected by the DCA and processes them using the anomaly and signature databases. This analysis and inspection is separated from the detection engine for fast performance via dedicated resources. The results are passed to the TDA for decision making.

4.5. Security and Network Management (SNM)

In response to decisions received from the TDA, an action can be triggered, e.g. block the threat and

Discussion

log its pattern and information in the anomaly database, or isolate the threat for further investigation.

4.6. Keep-Alive (KA)

This protocol maintains timers for all CCIPSs. When a CCIPS timer reaches zero, it sends a 'keep-alive' probe to its peers, who then respond with ACK packets to assert that they are active. Failure to receive a response to a keep-alive probe indicates a CCIPS system failure (e.g. due to an attack or hardware failure).

4.7. Cooperation Agent (CA)

This agent is responsible for the coordination and collaboration of the CCIPS signature and anomaly databases among all connected/participating CCIPSs. The cooperation interval can be scheduled or set to update on-the-fly whenever changes are made to the databases.

4.8. Administrator Interface Console (AIC)

This interface enables the CCIPS administrator to manage and access all CCIPS components. The AIC enables access to activity monitors, system logs, and the threat patterns in the anomaly database. The CCIPS administrator manages SNM actions associated with each decision made by the TDA via this console. This allows TDA decisions to be associated with an automated request to drop/block certain IP addresses and/or port numbers, or any other network security request.

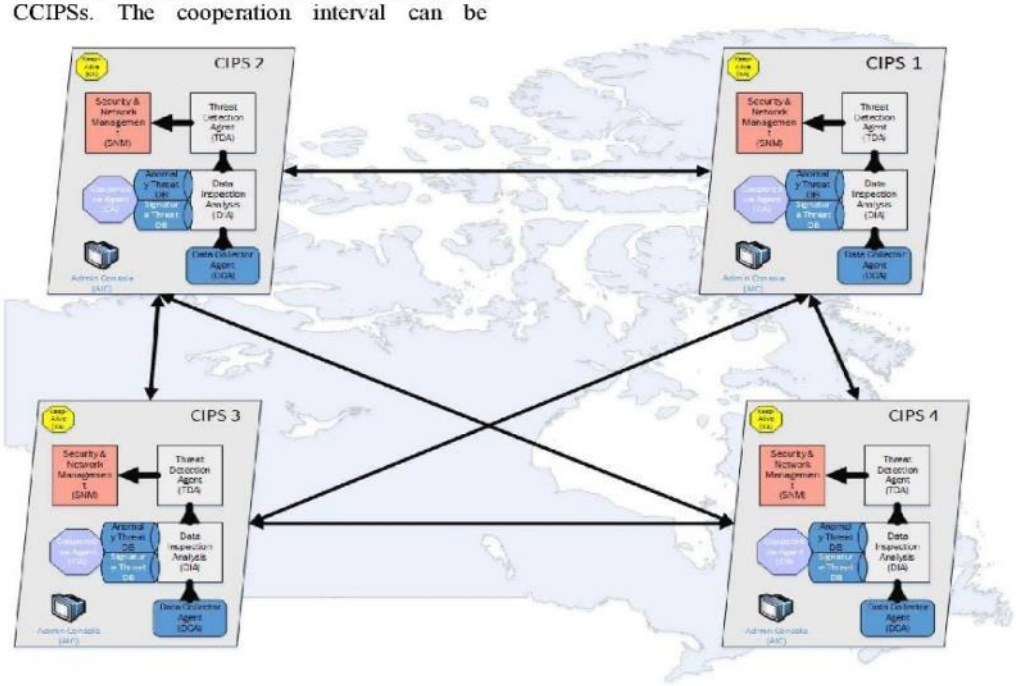


Figure 4 The Cooperative Cloud Intrusion Detection and Prevention System (CCIPS) distributed across the country.

5. Discussion

The proposed framework provides proactive intrusion detection which is applicable to the Infrastructure-a-a-Service (IaaS) cloud service model. This model is the foundation for cloud services and any security breach at this level will inevitably compromise the upper cloud service layers (e.g. PaaS and SaaS). Thus the focus here is the detection and prevention of threats to the IaaS layer.

Each cloud service provider has their own virtualization platform. The ability to embed CCIPS sensors into the layers of their infrastructure requires their cooperation and adoption of the CCIPS approach. Further, the implementation of large-scale CCIPS collaboration of CCIPS needs service provides to

exchange information and interoperate with each other.

The cooperation of threat knowledge (known attacks and unknown threats), among CIPS peers within the enterprise network or with other cloud services providers will contribute to better incident detection and prevention. This enhances cloud security and provides faster and more effective incident response.

Existing frameworks have an IDS in only one layer of the IaaS cloud service model. For example, Laniepce et al. [12] proposed an IDS for only one component in this service model. It was designed to protect the user virtual machines (supervisor). Other frameworks proposed in the literature either focus on one component in a service model or on a high level of integration (traditional IDS). Conversely, the proposed framework integrates intrusion detection in every component of the IaaS cloud service model. This provides comprehensive monitoring of all IaaS activities. It also takes proactive actions which enhances the security.

The CCIPS provides scalability so that multiple IaaS deployments can be monitored. These systems can collaborate regionally or globally as shown in Figure 4. This also brings high performance (HP) and high availability (HA) via additional Active-Backup CCIPSs configured to handle increased demand due to new IaaS layers. In addition, this framework allows for load-sharing and load-balancing of CCIPS activities.

If the proposed framework is adopted, cloud service providers will require additional resources such as virtual servers, load-balancing and load-sharing equipment, correlation agents, database servers, and related networking hardware. With new mandates, privacy laws and regulations, and the ever increasing concerns of governments and other agencies, cloud service providers must be proactive in addressing security issues. The solution identified in this paper requires that service providers invest in security infrastructure, but it can provide HA and HP, and interoperability among different IaaS platforms, and with other cloud service models (e.g. SaaS and PaaS).

6. Conclusion

Cloud computing is an attractive solution for those who seek IT flexibility and efficiency. Systems are being developed rapidly for the delivery of cloud services. With on-demand access on a pay-per-use basis, users can reduce capital costs by using customizable cloud services. It is predicted that many organization will migrate to cloud computing services [6]. However, the flexibility provided by cloud-based technologies results in security issues that may impede the adoption of cloud computing.

A security framework was proposed for the IaaS cloud computing service model to protect both users and providers from loss of services and resource access. This framework is based on an integration of recent intrusion detection and prevention technologies and National Institute of Standards and Technology (NIST) guidelines. It offers opportunities for the development of effective intrusion prevention systems (in terms of detection accuracy and proactive response mechanisms), to protect the cloud computing environment.

References

[1] Kaufman L.M., "*Data security in the world of cloud computing*", IEEE Security & Privacy, Vol. 7, No. 4, pp. 61-64, 2009.

[2] Foster I., Zhao Y., Raicu I., and Lu S., *"Cloud computing and grid computing 360-degree compared"*, Grid Computing Environments Workshop, IEEE, USA, pp.1-10, 2008.

[3] Lo C., Huang C., and Ku J., "*A cooperative intrusion prevention system framework for cloud computing networks*", International Conference on Parallel Processing Workshops, IEEE, USA, pp. 280-284, 2010.

[4] Peter M., and Grance T., *The NIST definition of cloud computing* (draft), NIST special publication 800 (145), 2011.

[5] Buecker A., Lodewijkx K., Moss H., Skapinetz K., and Waidner M., *Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security,* IBM Corp. p. 2, p. 7, p. 19, 2009.

[6] Frank Gens. New IDC IT Cloud Services Survey: Top Benefits and Challenges. http://blogs.idc.com/ie/?p=730. IDC eXchange, Last viewed (15-10-2013).

[7] International Data Corporation. http://blogs.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenges_2009.jpg, 2009. Last viewed (10-11-2013).

[8] Chaves D., Aparecida S., Becker Westphall C., and Rodrigo Lamin F., "*SLA perspective in security management for cloud computing*",

International Conference on Networking and Services, IEEE, Mexico, pp. 212-217, 2010.

[9] Stoneburner G., Goguen A., and Feringa A., *Risk management guide for information technology systems*, NIST special publication 800.30, 2002.

[10] Keiko H., David G. R., Fernández-Medina E., and Fernandez B., "*An analysis of security issues for cloud computing*", Journal of Internet Services and Applications, Vol. 4, No. 1, pp. 1-13, 2013.

[11] Farzad S., "*Cloud computing security threats and responses*", International Conference on Communication Software and Networks, IEEE, China, pp. 245-249, 2011.

[12] Laniepce S., Lacoste M., Kassi-Lahlou M., Bignon F., Lazri K., and Wailly A., "*Engineering intrusion prevention services for IaaS clouds: The way of the hypervisor*", International Symposium on Service Oriented System Engineering, IEEE, USA, p. 25-36, 2013.

[13] Yassin W., Udzir N. I., Muda, Z., Abdullah A., and Abdullah M. T., "*A cloud-based intrusion detection service framework*", International Conference on Cyber Security, Cyber Warfare and Digital Forensic, IEEE, Malaysia, pp. 213-218, 2012.

[14] Kenichi K., and Chiba S., "*HyperSpector: Virtual distributed monitoring environments for secure intrusion detection*", ACM/USENIX International Conference on Virtual Execution Environments, ACM, USA, pp. 197-207, 2005.

[15] Stiawan D., Abdullah A., and Yazid Idris M., "*The trends of intrusion prevention system network*", International Conference on Education Technology and Computer, IEEE, China, pp. V4-217-V4-221, 2010.

[16] Hai J., Xiang G., Zou D., Wu S., Zhao F., Min Li, and Zheng W., "*A VMM-based intrusion prevention system in cloud computing environment*", The Journal of Supercomputing, Vo. 66, No. 3, pp. 1133-1151, 2013.

[17] Saman Taghavi Z., Takabi H., and James B.D. J., "*DCDIDP: A distributed, collaborative, and data-driven intrusion detection and prevention framework for cloud computing environments*", International Conference on Collaborative Computing: Networking, Applications and Worksharing, IEEE, USA, pp. 332-341, 2011.

Chapter 3

Trusted CCIPS: A Trust Security Model for Cloud Services Based on a Collaborative Intrusion Detection and Prevention Framework

As published in *International Journal of Latest Trends in Computing*,
March 2014

This article appeared in Vol. 5, Issue. 1, published by *International Journal of Latest trends, Copyrighted to © ExcelingTech Publisher, UK*. The attached copy is furnished to the author for internal non-commercial research and education use, including for instructions of the authors institution and sharing with colleagues.
Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.
In most cases authors are permitted to post their version of the article to their personal websites or institutional repository. http://ojs.excelingtech.co.uk/

162
Int. J Latest Trends Computing
Vol-5 No. 1, March 2014

Trusted CCIPS: A Trust Security Model for Cloud Services Based on a Collaborative Intrusion Detection and Prevention Framework

Fahad F. Alruwaili[1] and T. Aaron Gulliver
Department of Electrical and Computer Engineering
University of Victoria, PO Box 1700, STN CSC
Victoria, BC V8W 2Y2, Canada
email: fruwaili@uvic.ca, agullive@ece.uvic.ca

***Abstract*—Recent advances in cloud computing services have resulted in a significant increase in the number of organizations adopting cloud service models. This raises Confidentiality, Integrity, and Availability (CIA) concerns as well as trust related issues, particularly when the cloud hosts sensitive infrastructure and applications. In addition, cloud service providers face many challenges in maintaining customer CIA. This paper considers the detection and prevention of threats by proposing a trust model based on a Cooperative Cloud Intrusion Prevention System (CCIPS) framework. This model is based on enhanced detection and prevention via signature and anomaly based data analysis. It is shown to provide high performance and high availability via a cooperative approach to security for infrastructure and application based cloud service models.**

***Keywords*—**Trust, Intrusion Detection, Intrusion Prevention, Security, Threats, Cloud Services.

[1]The research of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia

1. Introduction

Cloud computing has emerged as a new means of delivering information technology capabilities. Cloud computing resources are delivered on-demand as a service for customers via the internet. The reliable and stable high-speed internet provides the ideal environment for the rapid evolution of cloud services. The advantages of cloud computing include anytime, anywhere availability with dynamic scalability for customers at a fraction of the cost of a traditional data centre. However, these technological and economic benefits can be outweighed by trust issues such as whether cloud providers can adequately protect customer assets [1].

Cloud computing service models were originally developed based on performance, convenience, on-demand deployment, and functionality. As a consequence, Confidentiality, Integrity and Availability (CIA) were given low priority. The lack of an extensive investigation of these issues during the early stages of cloud service development resulted in insecurities amongst potential cloud users. They require answers to questions such as is their data physically segregated from our competitors, and is it securely protected against adversaries sharing the same cloud service (virtual resource). These and other security concerns have impeded the adoption of cloud services [2].

Table 1 shows the results of a recent survey by the International Information Systems Security Certification Consortium (ISC)² of the global information security workforce during September to December 2012 on trends and issues that affect IT professionals [7]. This shows that 89% of the over 12 thousand IT professionals who responded indicated that there remain considerable ambiguities in understanding cloud related risks. In addition, they reported that there is a lack of suitable standards and regulations with respect to information security and privacy practices and procedures [17].

Copyright © ExcelingTech, Pub, UK (http://excelingtech.co.uk/)

Table 1 The results of a 2013 $(ISC)^2$ survey of the global information security workforce on the skills required in dealing with cloud computing [7].

The core of cloud computing is the outsourcing of services so that customers (tenants) can manage their applications and/or hosted systems through internet-enabled Application Programming Interfaces (APIs). This multi-tenancy architecture is a fundamental aspect of cloud computing services. However, it also introduces privacy assurance and access control issues in cross-tenant resources. Cloud computing customers should have confidence that their service providers will employ proper data security and privacy measures. This will improve the trust and reputation of cloud service providers, and increase the use of their services [3].

Previously, we introduced a framework that protects the infrastructure layer of cloud computing services. This framework, called the Cooperative Cloud Intrusion Prevention System (CCIPS), can detect and prevent known and zero-day intrusions in a collaborative cloud infrastructure service model. The CCIPS framework is illustrated in Figure 2. The CCIPS monitors traffic in all Infrastructure as a Service (IaaS) system components. If an incident is detected by the Treat Detection Agent (TDA), a rule-based action triggers Security and Network Management (SNM) to generate an incident response. The TDA and SNM cooperate to validate, isolate, and remediate known and zero-day intrusions. Manual intervention by CCIPS administrators or cyber security analysts is kept to a minimum. The CCIPS allows administrators and forensic teams to investigate and react to an incident in real-time through the Administrator Interface Console (AIC) [4].

In this paper, a trust model is proposed for cloud customers that provides public knowledge and examination of security evaluation results. It is based on the performance metrics of the cooperative intrusion detection and prevention framework implemented in the infrastructure and application layers of the cloud computing environment. The infrastructure layer (IaaS) serves as the basis for cloud services and is the foundation layer for the upper cloud service layers (i.e., PaaS and SaaS). Incidents compromising this foundation layer will inevitability impact the higher layers and hence compromise the security and privacy of customer application systems and data. The focus here is on trust-based cloud intrusion detection and prevention. This will support cloud service providers in improving the reliability, performance, and accuracy of their intrusion detection and prevention systems in the SaaS and PaaS service models. The long term goal is to support business and government organizations to migrate their application software, operating system platforms, and infrastructure to trusted cloud computing providers.

The trust model developed here is an extension of the CCIPS framework with a focus on trust implementation in the cloud environment. The trusted CCIPS model is based on socio-technical system (STS) theory where the cloud society (e.g.

cloud customers and cloud auditors/assessors), is an integral component in building trust transparency and assessing the reputation of cloud service providers [12]. To ensure the consistency and correctness of this model, the National Institute of Standards and Technology (NIST) 800-53 R4 trustworthiness model should be integrated into the design process [13].

2. Cloud Customer Requirements and Motivation

Organizations wanting to outsource their infrastructure, platforms, and applications to cloud service providers should revise their organizational, legal and operational requirements prior to making any decisions. This will ensure that a set of requirements is defined which is suitable for the acquisition of cloud services [8]. Unfortunately, information security and privacy requirements are often partially or completely ignored. Even if the requirements are satisfied, the cloud service provider will control the hosted services, especially if Software-as-a-Service (SaaS) has been acquired. Consequently, an organization must either accept the risk of trusting the service provider or establish its own data centre, operating systems, and/or applications.

3. Problem Analysis

In this section, the concerns associated with transferring infrastructure and applications to cloud services are discussed, followed by relevant attack models. The three main security and privacy concerns in outsourcing to cloud computing services are [9]

- Cloud service providers may not have adequate intrusion detection and prevention policies to meet customer security requirements.
- Cloud service providers may not have adequate intrusion detection and prevention controls. This can lead to information confidentiality and integrity being compromised, i.e., loss of customer intellectual property (IP).
- Cloud service providers may not have adequate intrusion detection and prevention systems to prevent service losses. This may affect the availability of customer information.

In the IaaS cloud service model, most attacks compromise the network resources and system infrastructure [10]. These are usually denial of service (DoS) or distributed DoS (DDoS) attacks that cause the network resources and system infrastructure to be unavailable to cloud users and/or customers. This is typically achieved by an attack consuming large amounts of bandwidth, .e.g. TCP/SYN flood [10].

DoS and DDoS attacks can also affect PaaS and SaaS cloud service models by overloading software applications with excessive service requests (e.g. login requests, search and database lookups). These application level attacks are usually harder to detect since the connection has already been established and thus can appear to the security systems as legitimate traffic. Other examples of DoS and DDoS attacks include amplification that enables the attacker to generate a request with a larger response (e.g. amplification of Domain Name Server (DNS) requests for large TXT records and HTTP GET flood requests for large image files). This will slow cloud service performance and eventually disrupt services (system unavailable or cannot be reached) [9], [10].

The goal of this paper is to address the trust concerns that potential cloud customers (tenants) face before entering into an agreement with a cloud service provider. Typically, potential customers have insufficient information about cloud service providers. In particular, whether adequate and resilient information security and privacy controls have been implemented. Consequently, customers often have no option but to accept the risks associated with transferring to a cloud service provider [6]. However, insufficient information about the security and privacy services cloud service providers offer can be partially mitigated by detailed service level agreements (SLAs) and detailed meetings.

We strongly suggest that customers address any security and privacy concerns prior to acquiring cloud services. By combining trust and reputation systems with SLAs, cloud customers can be confident in their choices. Solutions have been

proposed to address SLA requirements in cloud computing [1], [5]. However, the focus here is to leverage the trust relationship between cloud service providers and their current and future tenants to ensure continual evaluation, improvement and investment in intrusion detection and prevention systems.

4. Related Work

Establishing a trust model in a cloud environment is a complex problem. Ideally this should be a collaboration between industry practitioners and academic researchers [6].

Beth et al. [14] proposed a trust model for distributed open networks. This model was defined based on the direct trust for the link established between two entities. This trust is determined by positive/negative experience recommendations from the entities.

Li et al. [15] suggested a cross-cloud trust model that identifies two roles (customer and service provider) in the cloud domain (a set of cloud resources). A trust agent is responsible for establishing a trusted relationship between cloud customers and cloud resources based on the specified constraints.

Pawar et al. [5] proposed an approach to trust that employs opinions on cloud service providers. These are based on compliance with SLA agreements, service provider satisfaction ratings, and service provider behaviour.

Shen et al. [16] proposed a Trusted Computing Platform (TCP) which can be integrated into a cloud computing system. This platform is used to provide security to cloud services such as authentication, role-based access and data confidentiality. It is designed to provide end-to-end service assurance.

Most of the proposed approaches to trust have focused on open systems such as e-commerce, peer to peer, and multi-agent systems. Conversely, research into trust for services such as the SaaS cloud service model has been limited [4]. In this paper, we consider existing approaches to cloud trust and reputation. Then a new trust model is proposed which includes the performance of the cloud intrusion detection and prevention systems of service providers. This allows customers to make informed decisions in choosing and retaining cloud service providers.

5. Objectives

The aim is to devise a robust trusted cloud computing environment. This trust is based on the system detection and prevention of malware, viruses, and online attacks. This focus on detecting known and unknown attacks and viruses is not to reveal deficiencies in the protection provided by cloud service providers, but rather to leverage trust and identify best practices in the cloud community. This will assist customers in choosing a cloud service provider, as well as service providers in improving their security.

It is assumed that cloud service providers will allow customers and trusted cloud auditors to review, criticize, and evaluate the performance of their security and privacy systems. The advantage for providers will be an increase in public trust, quality of service, and cloud service adoption. This can be achieved by soliciting opinions and feedback from current customers and trusted cloud assessors/auditors on the security and privacy controls and policies implemented by service providers.

6. Trusted CCIPS

This section outlines the extension of our cloud intrusion detection and prevention framework to provide a trust security model.

6.1. Trust Definition

The word ‘trust’ has a variety of meanings depending on the application. Two commonly used definitions of trust are reliability-trust and decision-trust [5]. Here, we propose a trust model based on the reliability of the infrastructure-CCIPS and application-CCIPS systems. Trust is subjective and can be considered as an expectation that an individual will perform a given action which affects the welfare of others [6]. For example, cloud customer A may expect that cloud service provider X will perform acceptable and adequate actions to

protect against security incidents and mitigate the resulting effects.

NIST [13] defines trustworthiness in information systems as follows.

> "The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation."

The proposed trust model is based on internal and cross layer trust where the higher layer CCIPS (application-CCIPS) trusts the intrusion database and system log of the lower layer (i.e., infrastructure-CCIPS), and vice versa. This model provides information to assist cloud customers in making informed decisions on cloud service providers. This information should be transparent and indicate the ability of cloud provider CCIPS systems to withstand cyber and internal attacks.

6.2. Scalable Cloud Cooperative Intrusion Prevention (CCIPS) Architecture

The CCIPS framework [4] not only monitors and detects known threats but also monitors behavioural changes due to zero-day threats and unauthorized or suspicious behaviour. In this paper, we extend this framework to include the upper cloud services (applications). Thus, the new framework has two modules as described below.

- *Infrastructure-CCIPS*: to capture and analyse data from the cloud infrastructure components (e.g., networks, servers, storage, and operating systems). The infrastructure-CCIPS searches for patterns that indicate malicious activities on network services (e.g., very high payload or traffic levels), and infrastructure components to detect and prevent service outages.
- *Application-CCIPS:* to capture and analyse data from cloud application level components such as software, Application Programming Interfaces (APIs), and other web- or application-enabled interfaces. The application-CCIPS closely monitors the application configuration status in order to identify suspicious activities (e.g. compromised software, unauthorized modification of configuration files, and rogue processes).

In order to intercept all packets in the service stack of the cloud environment, the CCIPS must be placed inside each cloud service layer. In this way, the CCIPS can monitor all processes and transactions and compare them against rules and policies defined in the threat databases.

6.3. Socio-Technical Systems

The trust model concerns all people, architectures, and technologies involved in cloud services. Socio-Technical System (STS) theory is used to allow cloud customers and service providers to collaborate in evaluating the trust of CCIPS systems. The objectives are to maximize transparency and trustworthiness. As shown in Figure 1, the STS is composed of two distinct but interacting (cloud society and cloud service providers) groups that participate in determining trust. This trusted-CCIPS model is based on shared knowledge of past and current performance cloud service provider security. The model attributes are given in Table 1.

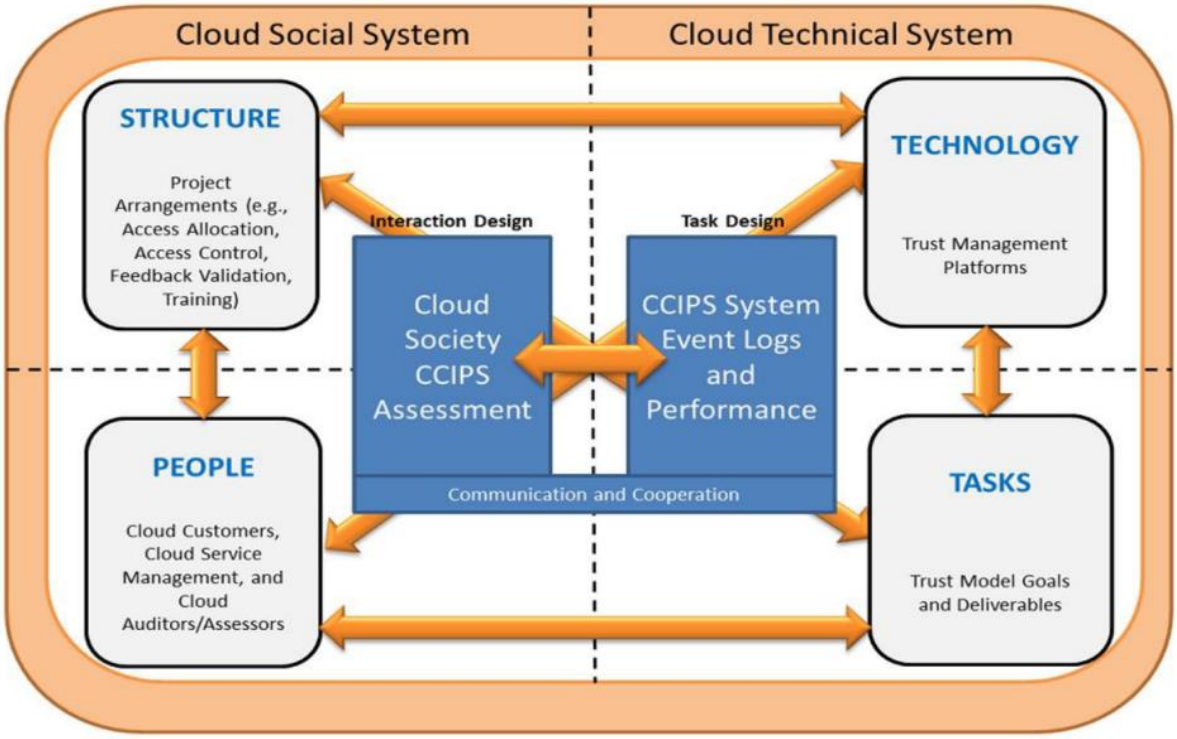


Figure 1 The STS based trust model.

Attribute	Trusted Collaborative Cloud Intrusion Prevention System (CCIPS) Model
Goal	Improve information security and maximize cloud customer satisfaction
Solution requirements	Satisfaction, trustworthiness, and reputation
Tacit knowledge	CCIPS assessment decisions by the cloud society
Design method	Synthesize a trusted-CCIPS model

Table 1 The trust model attributes

6.4. The Trusted CCIPS Model

There are two intrinsic components to the proposed trust model as described below.

6.4.1. Trust among CCIPS Systems

The first component is a trust collaboration between CCIPS systems via event logs and the threat databases of the cloud service layers. These are as follows:

Local Trust: Trust between cloud computing service layers. For example, an incident which occurs in the IaaS layer can be shared with the CCIPS in the application layer to eliminate and/or minimize the impact of the incident.

Global Trust: Trust among intra-connected CCIPSs within the infrastructure of a cloud service provider can be achieved by sharing the databases of known and new threats. This sharing can be performed both locally and globally to increase the accuracy and robustness of the intrusion detection and response mechanism.

Public Trust: To enable transparency in the CCIPS performance evaluation, all closed incidents will be filtered and made available for public evaluation, reference purposes, and customer reporting and awareness. An independent trusted cloud service auditor can be granted access to view and monitor CCIPS event logs to ensure compliance with security agreements and for security system evaluation.

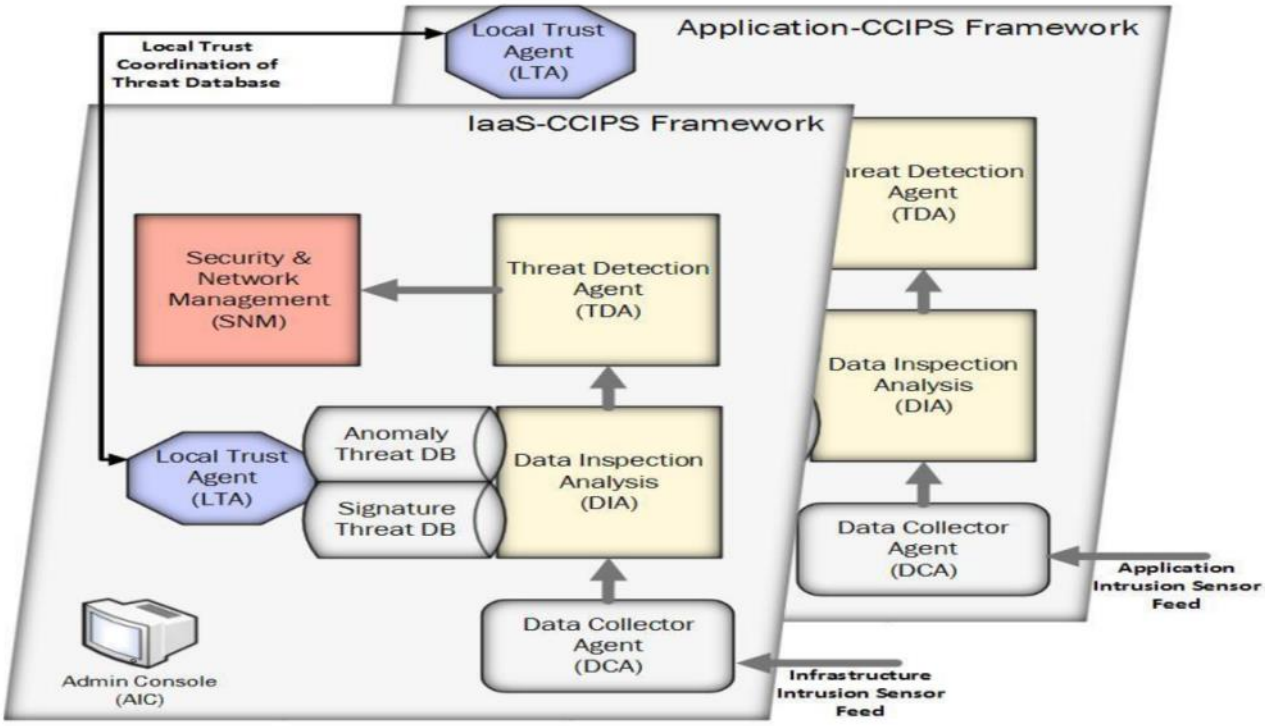


Figure 2 The IaaS and application CCIPS framework.

6.4.2. *Client Trusted Assessment*

The second component of the trust model relies on input from cloud customers and trusted third party cloud service security auditors/assessors. The resulting evaluations are based on both customer experience and opinions on how the hosted infrastructure, platforms, applications, and data can withstand attacks. The evaluations are also dependent on continuous and rigorous assessment by the auditors/assessors. These third party cloud assessment organization must be recognized and accredited to undertake comprehensive vulnerability and penetration testing (e.g. network and infrastructure stress testing, application testing, web service testing, and source code auditing), and benchmarking the results using approved cloud security standards, controls and guidelines.

To ensure the credibility and accuracy of the assessments, each assessor is given a unique and secret ID to access the trust management system. The system must provide non-repudiation by ensuring an assessor cannot deny the authenticity of a submitted evaluation.

The final assessment results are published and made available to the public including potential cloud customers. This process is repeated regularly according to the agreements between cloud stakeholders. These formal periodic reviews should take place weekly, bimonthly, monthly, or after every critical incident.

6.5. The Trust Model Structure

The trusted-CCIPS system model is presented in Figure 2. It is isolated from the core operations of the CCIPS systems to minimize the overhead and maximize the security and transparency of the model.

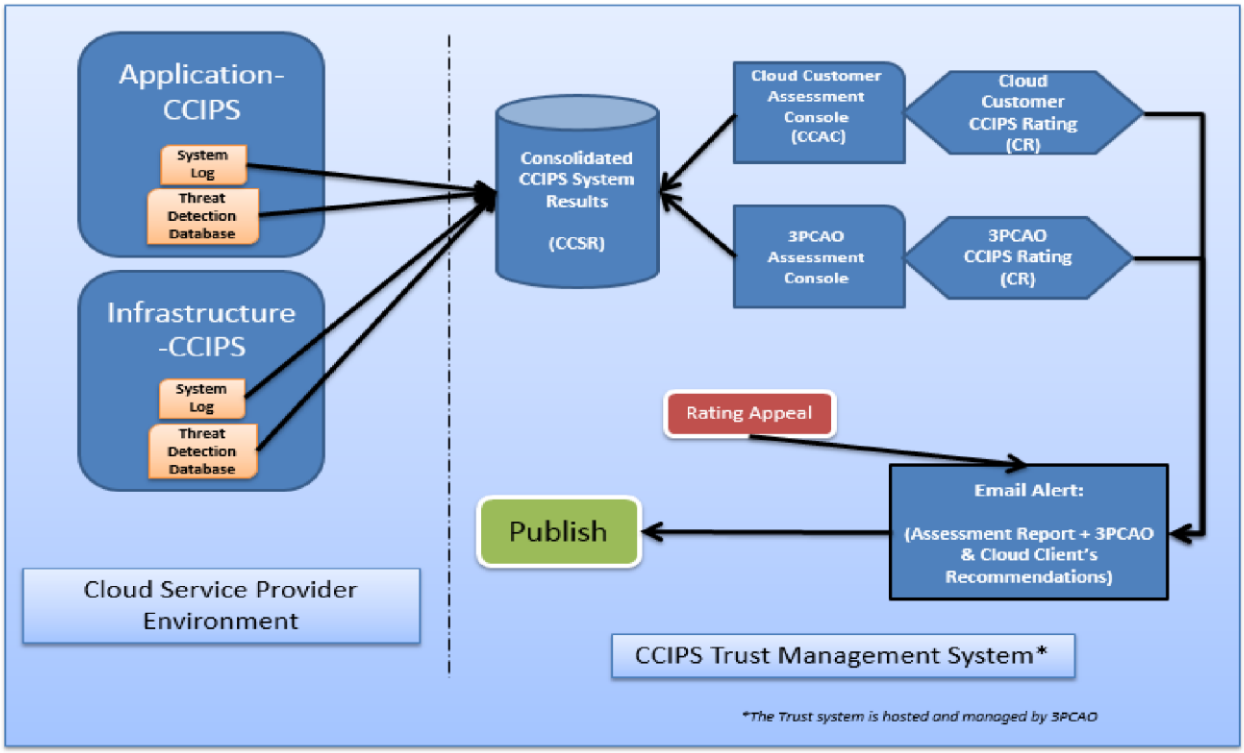


Figure 3 The proposed trusted CCIPS model.

The trust model consists of the following components.

6.5.1 *Consolidated CCIPS System Results (CCSR):* This CCSR allows cloud customers and assessors to access (read only), the CCIPS log files (e.g. running processes, user logins/logouts, shutdowns, and restarts), event logs, and threat databases. This can be done in real-time or via archived data. The CCSR provides real time cloning of all CCIPS system event logs and threat databases to reduce the processing overhead when multiple cloud customers are monitoring the system.

6.5.2 *Cloud Customer Assessment Console (CCAC):* The CCAC is a feedback/assessment console that enables customers to view CCIPS performance on the hosted system (e.g. infrastructure, platform, application and data). Customers will not be able to view the performance of other hosted systems due to privacy requirements. An assessment is given a unique identification code that links the customer, hosted system, and questionnaire or report

Discussion

to ensure the validity of the information provided.

6.5.3 *Third Party Cloud Assessment Organization (3PCAO):* The 3PCAO consists of trusted third parties who will be able to view and assess the operation of all CCIPS systems (e.g. system files and configurations, setup and design, and performance history). They will provide evaluations and recommendations to improve cloud service provider security systems.

6.5.4 *CCIPS Rating (CR):* The CR is based on predefined CCIPS performance factors. These will be made available publically using the following scale:

(5) Exceptional
(4) Exceeds Expectations
(3) Satisfactory
(2) Fair, security needs minor improvements
(1) Unacceptable, security requires major improvements.

6.5.5 Alerts and Recommendations: The alerts and recommendations are secure reports delivered after the assessments have been completed. Both involved parties (e.g. cloud service providers and customers), will be provided with draft reports followed by final reports, typically via email. Non-repudiation of these reports must be ensured. In addition, they should be encrypted to ensure the integrity and confidentiality of the assessments.

These reports may also contain recommendations from customers and assessors to improve the CCIPS system. These will typically be based on incident responses and/or proactive steps against unforeseen cyber threats.

6.5.6 *Rating Appeal:* This allows service providers to appeal the ratings given by cloud customers and/or assessors. This may result in a revision of the initial CCIPS assessment. This process must be completed before publication of the final report.

6.5.7 *Rating Publication:* The final step is publication of the CCIPS ratings for public viewing.

7. Discussion

In this section, the advantages of the proposed trust model discussed based on the objectives identified in Section 5. The proposed trust model is based on collaboration between infrastructure-CCIPS and application-CCIPS to provide performance metrics for cloud data protection (storage, processing, and transmission). This collaboration can be done both locally and globally with participation by remote cloud systems and/or cloud service providers. The benefit of local and global collaboration is increased accuracy and consistency of the threat databases. The CCIPS framework allows scalability to better capture, evaluate, and protect cloud services against online and/or internal threats.

The approach presented in this paper complements existing cloud computing trust solutions. It differs from current approaches as it is based on CCIPS evaluation by cloud customers and 3PCAO assessors who have complementary experience and knowledge of the security performance of cloud service providers. The evaluations and assessments are based on the ability of the infrastructure CCIPS and application CCIPS of cloud service providers to adequately protect cloud services and customer data from unauthorized access, cyber and insider attacks, and malicious acts. In addition, the trust model indicates if cloud service providers have exercised due diligence and due care in the implementation and support of their intrusion detection and prevention systems.

The proposed extension of the CCIPS framework enables global and local collaboration of signature and anomaly databases and system logs to improve cloud incident response time, accuracy, and

efficiency. The trust model extension of this framework supports transparency and promotes competition among cloud service providers to deliver quality services. While the trusted CCIPS model can be developed and managed by cloud service providers, it is recommended that at least two trusted third party organizations have administration access to the trusted CCIPS systems. This helps protect against fraudulent results being reported, which improves the transparency and reliability.

8. Conclusion

There is a great need to address the security and privacy concerns and challenges in cloud service models [6]. Proper cloud information security and incident management is vital to the success of cloud service providers. However, it is inevitable that the number and sophistication of cyber attacks and malware will increase. Thus it is important that information security practitioners and researchers contribute to solving cloud information security and privacy issues [22], [23].

Cloud service providers must invest in the security and protection of cloud customer data and intellectual property. Continual improvements in delivering secure and private cloud infrastructure and applications will aid in building a robust and trusted cloud environment. This is not only feasible but also desirable by the cloud community and service providers to address customer security concerns. Moreover, the Federal Risk and Authorization Management Program (FedRAMP) recently proposed legislation to enforce cloud service providers to undergo 3PCAO assessment in order to meet the minimal security requirements outlined by the Federal Information Security Management Act (FISMA) [18-21]. This legislation will encourage cloud service providers to invest in a secure and reliable cloud infrastructure. This in conjunction with the proposed trust model will increase customer confidence and trust in adopting cloud services.

The proposed trust model is an extension of the scalable CCIPS framework to build security, privacy, and trust in cloud computing environments. This model enables cloud customers and accredited cloud assessment organizations (3PCAO) to evaluate the efficiency and effectiveness of incident response programs employed by cloud providers. They can then determine if service providers are in compliance with cloud customer Service Level Agreement (SLA) and contractual obligations.

References

[1] M. Alhamad, T. Dillon, and E. Chang, *"SLA-based trust model for cloud computing."* IEEE International Conference on Network-Based Information Systems, pp. 321-324, 2010.

[2] S. Hiroyuki, A. Kanai, and S. Tanimoto, *"A cloud trust model in a security aware cloud."* IEEE/IPSJ International Symposium on Applications and the Internet, pp. 121-124, 2010.

[3] T. Bo and R. Sandhu, *"Cross-tenant trust models in cloud computing."* IEEE International Conference on Information Reuse and Integration, pp. 129-136, 2013.

[4] F. F. Alruwaili, and T.A. Gulliver, "*CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services.*" International Journal of Latest Trends in Computing, December 2013.

[5] P. S. Pawar, M. Rajarajan, S. Krishnan Nair, and A. Zisman, *"Trust model for optimized cloud services."* Trust Management VI, IFIP Advances in Information and Communication Technology, Springer, Berlin, Vol. 374, pp. 97-112, 2012.

[6] I. A. Abbadi and A. Martin, *"Trust in the Cloud."* Journal of Information Security and Applications, Vol. 16, No. 3, pp. 108-114, 2011.

[7] M. Suby, Global Information Security Workforce Study. Frost & Sullivan Market Study. Accessed from https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf, Last viewed (15-01-2014).

[8] W. Janson and T. Grance,*"Guidelines on Security and Privacy in Public Cloud Computing."* NIST Publication 800-144, 2011. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf, Last viewed (2-02-2014).

[9] Quarterly Global DDoS Attack Report released by Prolexic, Apr 2013, http://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q1/pr.html, Last viewed (27-01-2014).

[10] Prolexic, DoS and DDoS Glossary of Terms, http://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q1/pr.html. Last viewed (27-01-2014).

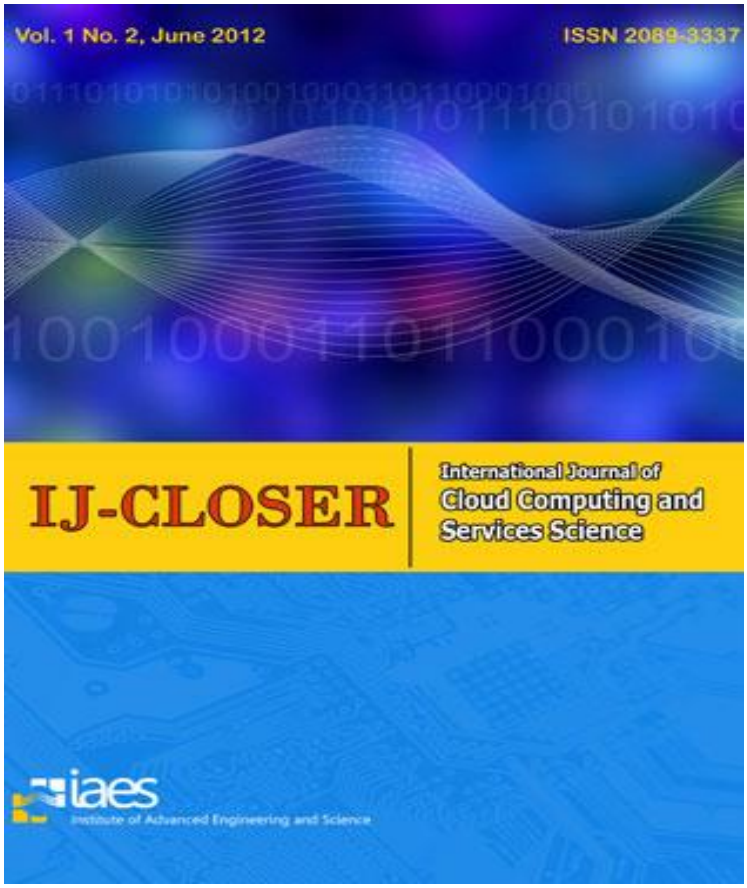
Chapter 4

[11] S. Farzad, *"Cloud computing security threats and responses."* IEEE International Conference on Communication Software and Networks, pp. 245-249, 2011.
[12] A. Serkan, *"Theories Used in Information Security Research: Survey and Agenda."* Handbook of Research on Social and Organizational Liabilities in Information Security, Ch. 17, pp. 279-292, 2009.
[13] NIST Special Publication 800-53A: Guide to Security and Privacy Controls, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, Last viewed (22-01-2014).
[14] T. Beth, M. Borcherding, and B. Klein, *"Valuation of trust in open networks."* Proceedings of European Symposium on Research in Computer Security (ESORICS), Lecture Notes in Computer Science, Vol. 874, Springer-Verlag, Berlin, pp. 3-18, 1994.
[15] L. Wenjuan and L. Ping, *"Trust model to enhance security and interoperability of cloud environment."* Proceedings of International Conference on Cloud Computing, Lecture Notes in Computer Science, Vol. 5931, Springer, Berlin, pp. 69-79, 2009.
[16] S. Zhidong, L. Li, F. Yan, and X. Wu, *"Cloud computing system based on trusted computing platform."* IEEE International Conference on Intelligent Computation Technology and Automation, 2010.
[17] $(ISC)^2$, Shortage of Skilled Cyber Security Professionals Causing Economic Ripple Effect across the Globe, http://www.prweb.com/releases/2013/2/prweb10464398.htm, Last viewed (20-01-2014).
[18] The Federal Risk and Authorization Management Program (FedRAMP), http://cloud.cio.gov/fedramp, Last viewed (04-02-2014).
[19] M. Kozlovszky, M. Trocsik, T. Schubert, and V. Póserné, *"IaaS type cloud infrastructure assessment and monitoring."* IEEE International Convention on Information and Communication Technology Electronics and Microelectronics, pp. 249-252, 2013.
[20] Federal Information Security Management Act (FISMA), http://csrc.nist.gov/drivers/documents/FISMA-final.pdf, Last viewed (15-01-2014).
[21] D. E. Issa, Library of Congress, Federal Information Security Amendments Act of 2013, http://thomas.loc.gov/cgi-bin/bdquery/z?d113:h.r.1163:/, Last viewed (01-02-2014).
[22] M. L. Kaufman, *"Can public-cloud security meet its unique challenges?." IEEE* Security and Privacy, Vol. 8, No. 4, pp. 55-57, 2010.
[23] Top Threats to Cloud Computing. March 2010. Cloud Security Alliance. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Last viewed (27-03-2014).

Chapter 4

SOCaaS: Security Operations Center as a Service for Cloud Computing Environments

As published in *International Journal of Cloud Computing and Services Science*, April 2014



This article appeared in Vol. 3, Issue. 2, published by *International Journal of Cloud Computing and Services Science Copyrighted to © 2012 IAES Institute of Advanced Engineering. The attached* copy is furnished to the author for internal non-commercial research and education use, including for instructions of the authors institution and sharing with colleagues.
Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.
In most cases authors are permitted to post their version of the article to their personal websites or institutional repository. http://www.iaesjournal.com/

Institute of Advanced Engineering and Science

International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.3, No.2, April 2014, pp. 87~96
ISSN: 2089-3337

SOCaaS: Security Operations Center as a Service for Cloud Computing Environments

Fahad F. Alruwaili*, T. Aaron Gulliver*
* Department of Electrical and Computer Engineering
University of Victoria, PO Box 1700, STN CSC
Victoria, BC V8W 2Y2, Canada
Email: fruwaili@uvic.ca, agullive@ece.uvic.ca

Article Info

Article history:

Accepted Apr 10th, 2014

Keyword:

Security Operations Centre (SOC), Security Incident and Event Management (SIEM), Threats, Cloud Security Services, Service Level Agreement (SLA), Cloud Governance.

ABSTRACT

The management of information security operations is a complex task, especially in a cloud environment. The cloud service layers and multi-tenancy virtual architecture create a complex environment in which to develop and manage an information security incident management and compliance program. This paper presents a novel security operations center (SOC) framework as a service for cloud service providers and customers. The goal is to protect cloud services against new and existing attacks as well as comply with security policies and regulatory requirements. The SOCaaS design is based on multi-governance and defense in depth models and fits within the multi-tenancy cloud services. A SOCaaS provider is a trusted entity that collects event and system logs from cloud systems to ensure proactive incident management and compliance with regulations. The proposed approach provides better managed services for customers wanting to outsource their information security operations to attain reliable, transparent, and efficient cloud security and privacy.

Copyright © 2014 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Fahad F. Alruwaili
Department of Electrical and Computer Engineering
University of Victoria, PO Box 1700, STN CSC
Victoria, BC V8W 2Y2, Canada
Email: fruwaili@uvic.ca

1. INTRODUCTION

Cloud computing resources are delivered on-demand as a service for customers over the internet. They can be constructed from multiple interconnected components such as virtualized hardware, operating systems, services and tools, platform components, and customizable software application [1]. This increases the complexity of cloud security services and their management. Thus, new techniques must be developed to provide efficient and reliable security for cloud computing environments [2].

When cloud computing service models were first developed, the focus was on performance, convenience, on-demand deployment, and functionality. Conversely, topics such as confidentiality, integrity and availability (CIA) were given low priority [3]. However, in [4] the authors show that there are significant costs associated with cyber attacks due to lost productivity, revenue and customer trust. In addition, a survey on the global state of information security [5] found that the financial losses, and lost intellectual property and company reputation as a result of cyber attacks can be substantial. Table 1 shows the results of a 2011 survey of 450 senior IT and business decision-makers on cloud adoption and trends by the Cloud Industry Forum (CIF) [6]. This shows that the top 4 issues in the cloud environment are data security at 64%, data privacy at 62%, and cloud availability and reliability.

Cloud services are delivered via the internet and are accessible anywhere, anytime. Thus these services are open to cyber attacks. In this paper, a security operation centre as a service (SOCaaS) is proposed for cloud service providers and customers to provide information security assurance and event management. It is based on the aggregation of events and logs from cloud security devices and systems. The infrastructure layer as a service (IaaS), platform layer as a service (PaaS), and software layer as a service (SaaS), typically have security devices deployed by the cloud provider. For example, a security device for intrusion detection and prevention can be embedded in each cloud layer [7]. It is expected that service providers will employ multiple security devices such as firewalls, identity management, proxy servers, antivirus software, encryption devices, and network analyzers. These security devices report events to the SOCaaS as the main source of data. The events are stored in a relational database for threat detection and analysis purposes. Events are gathered via SOCaaS system agents deployed in each cloud security device. The SOCaaS system aids cloud service providers in improving the reliability, performance, and accuracy of their security devices. The long term goal of SOCaaS is to support business and government organizations in migrating their application software, operating system platforms, and infrastructure to robust and secure cloud computing environments.

Table 1. Cloud Industry Forum Cloud Adoption and Trends Survey 2011 [6]

What are your most significant concerns, if any, about the adoption of cloud in your business?

Only asked of respondents who either currently use cloud or will do at some point in the future	Total	No. employees Fewer than 20	20-200	More than 200
Data security	**64%**	62%	61%	68%
Data privacy	**62%**	68%	61%	60%
Dependency upon internet access	**50%**	53%	58%	42%
Confidence in the reliability of the vendors	**38%**	32%	38%	41%
Contract lock-in	**35%**	30%	43%	30%
Cost of change/migration	**32%**	27%	35%	33%
Contractual liability for services if SLA's are missed	**31%**	16%	38%	33%
Confidence in knowing who to choose to supply service	**28%**	27%	29%	28%
Confidence in the vendors business capability	**24%**	16%	25%	26%
Confidence in the clarity of charges (ie will they be cheap on-prem)	**22%**	16%	26%	21%
Lack of business case to need cloud service	**21%**	11%	27%	22%
Base	**323**	73	112	95

The SOCaaS framework developed here is based on information security management [8], and computer security [9] models, both of which are described in detail in the next section. In addition, this framework conforms to the recommendations outlined by the Cloud Security Alliance (CSA) in category#7 [10]. CSA category#7 provides guidelines on the design and deployment of information security and event management services for cloud based networks, infrastructure and applications.

2. THE SOCaaS CONCEPT

The SOCaaS information security management model employs the best practices recommendations described below:

- *Information Security Management Model* [8]

  The SOCaaS framework is based on an information security management model where multiple system components are connected to all security devices in the cloud provider infrastructure and application domain. These devices are managed based on a predefined set of rules and policies shared with and agreed upon by the cloud customers. The SOCaaS obtains logs in the cloud provider domain, analyses, and correlates them in order to detect threats and predict uncertain events.

- *The Cloud Security Model*

  Straub [9], proposed a computer security model which is based on deterrence theory adopted from the discipline of criminology [11]. This security model has three layers. Within the SOcaaS framework, the first layer is a deterrents layer which employs policies defining acceptable and unacceptable behaviour in the cloud environment. Figure 1 shows this as the first layer on the left, with the other layers being prevention and detection of cloud abuse. The second layer prevents violations of rules and policies and cloud abuse. The third layer detects any deviations from these rules and cloud abuse through continuous monitoring and system audits. The goal is to discourage abuse of the system. Cloud abuse is defined as unauthorized and deliberate misuse of the cloud infrastructure by individuals and/or processes.

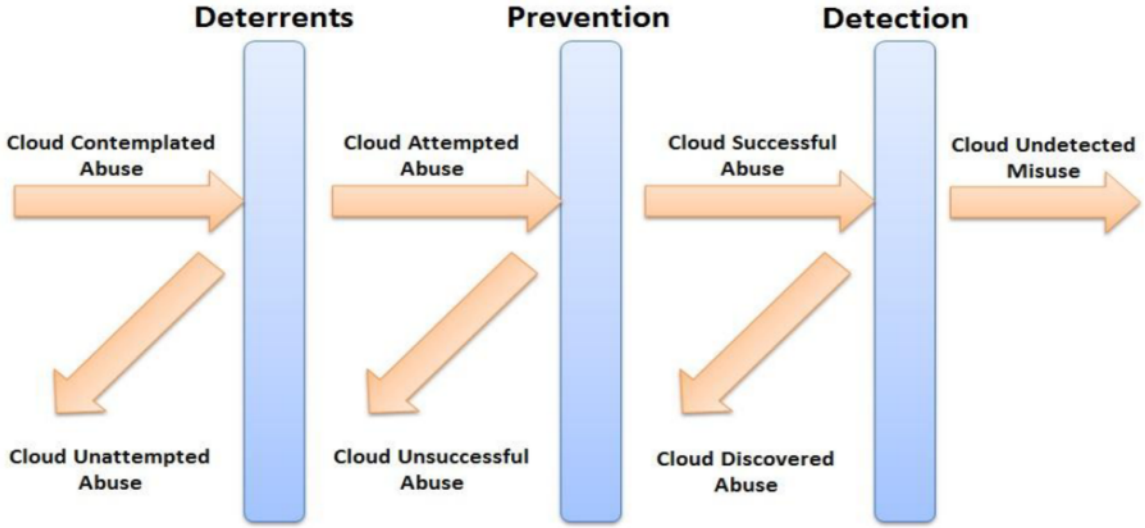


Figure 1. The cloud computer security model.

3. RELATED WORK

Establishing a security operations centre (SOC) in a cloud environment is a new approach to providing information security and event management to cloud services. The Cloud Security Alliance (CSA) [2] professionals and researchers have introduced the concept of Security-as-a-Service (SECaaS) to cloud services. They developed a set of requirements, and discussed implementation considerations and concerns. However, the recommendations provided did not specify a specific model to implement SOC in a cloud computing environment.

Probst et al. [12] suggested an automated evaluation of cloud security mechanisms and their efficiency. The focus was on evaluating access control and intrusion detection systems, which is just a part of the overall cloud risk management and assessment process. Further, their approach is limited to the cloud computing infrastructure.

In [13] the authors discussed the suitability of security-as-a-service (SaaS) for critical cloud information infrastructure services. They proposed a model to integrate traditional security solutions into a cloud infrastructure. However, their model only provides a high level description and does not provide any details of the implementation of the SOC in the cloud infrastructure or application layer.

Marty [14] presented a cloud logging framework and guidelines to provide a proactive approach to logging. This approach provides proactive information and system logging to ensure that the data needed for forensic investigation is available. While this is considered a main component of a SOC, it is limited to post event and reverse engineering analysis.

In [15], the authors introduced SECaaS using a service oriented architecture (SOA) to allow cloud customers to have more control over hosted services. A user-centric approach was employed to allow users to choose security services and monitor the status of their applications and data in the cloud environment. However, their architecture is limited to access control settings and some security settings in the chosen cloud service model (IaaS, PaaS, or SaaS).

Montesino et al. [16] reviewed security controls recommended by known standards such as ISO/IEC 27001 and NIST SP 800-35. They determined that 30% of the controls can be automated. They proposed a security information and event management (SIEM) framework to automate these security controls. They did not consider the application of their framework to the multi-layer/multi-tenancy architecture of a cloud computing environment. Further, 70% of the security controls are excluded which may leave the cloud environment vulnerable to attack.

4. OBJECTIVES

The aim of this paper is to devise a robust cloud security information and event management system. The SOCaaS is based on the aggregation of events from cloud security devices and applications. The collected events and system logs will be analyzed against an up-to-date cyber intelligence database to identify matching or relevant patterns. The SOCaaS oversights the security devices provided by cloud service suppliers. Periodic reports will be distributed to provide in depth comments and reports based on an analysis of this data, Forensic investigation should be conducted to identify threats affecting the cloud provider/customer. Note a single security device (e.g., a firewall), has limited information and thus may fail to detect and/or prevent cyber attacks. The goal here is not to expose deficiencies in the internal information security management of a cloud provider, but rather to leverage best practices in security operations and event management within the cloud community.

It is assumed that cloud service providers will allow the SOCaaS provider to deploy SOCaaS agents in their security devices for the purposes of collecting system events. It is also assumed that cloud service providers will allow the SOCaaS system to respond to an event that might require a change in a security device. The advantage for providers is an increase in public trust, service quality, and cloud service adoption. This is achieved by allowing customers to employ SOCaaS to oversee their hosted cloud services and provide real time security assurance.

5. SECURITY OPERATION CENTRE AS A SERVICE (SOCaaS)

This section first provides a definition of cloud events, the SOCaaS operational process is then disccused, and finally the proposed SOCaaS framework is described .

a. Event Definition

Cloud events can be classified into the following categories:

- *Violation of compliance policy:* detection of a violation of a defined set of rules (e.g. a user used a 128 bit encryption link instead of a 256 bit link to access a given cloud resource).
- *System configuration change:* an alert of a change in the configuration settings of cloud servers, applications, software, storage, or network components (e.g., auto-backup has been rescheduled from daily to once a week which can be a normal or unacceptable change based on the rules in the SOCaaS event database and/or the cloud security device/system).
- *Service vulnerability:* detection of a weakness in a cloud service that has been exploited to gain unauthorized access.
- *Compromised identity:* detection that personal information has been misused and/or stolen. (e.g. the credentials of a cloud user with access from a given location are used to access cloud services from a different location).
- *Data breach:* detection of a disclosure and/or data leak (spill) of sensitive, protected, or confidential cloud information by an unauthorized individual or process.
- *User Activity:* detection of user access to unauthorized virtual resources or has logged in a prohibited hours. Events can be triggered if a user exceeds his/her network or processing defined utilization permit. In addition, events can be triggered if a user tried to install unauthorized software application.
- *Attacks:* detection of a network attack such as distributed denial of service (DDoS), or web based attack such as SQL injection.

- *Malware infection:* detection of malware such as a virus, worm, or Trojan that slows cloud applications, corrupts system files, consumes cloud storage by self-replicating, or installs a backdoor for unauthorized access.

The event categories above are non-exhaustive. Detailed event definitions, categorization, and prioritization, must be developed and agreed upon by the cloud customers, service providers, and SOCaaS monitoring entity.

b. SOCaaS Operational Process

The key to an effective security operations centre is the event detection and analysis timeframe (i.e., time to detect, analyz, and repond). The faster the detection and analysis process, the better and more effective the SOCaaS system will be. The number of false positive and false negative events should also be kept low to ensure SOCaaS detection accuracy.

Figure 2 presents the timeline from event detection to response decisions, event research and analysis, and reporting. For example, the SOCaaS system detects a distributed denial of service (DDoS) attack against cloud customer 'A', which is a web server. After the initial correlation analysis, the system responds to block all active connections initiating the DDoS attack. If needed, the system can annotate the event for further investigation. Then the advanced event research and forensic analysis traces back to the origin of the attack. Finally, the corresponding patterns are used to update the system threat database, and the final report is distributed.

Figure 2. The SOCaaS operational process timeline.

c. SOCaaS Framework

The proposed Security Operation Centre as a Service (SOCaaS) framework is designed to provide comprehensive information security and event management for all cloud devices and applications. The correlation of all events and logs aggregated from all the security devices increases the likelihood of detecting and preventing attacks and threats compared to events and logs aggregated from one or few devices. This framework not only provides comprehensive cloud protection but also, assists in enforcing compliance and policy requirements. On demand event reports are provided for auditors from cloud service providers and customers in order to assess the process. Compliance and audit reports can also be used by external auditing agencies to verify adherence to regulatory standards and requirements, and for certification purposes. Law enforcement agencies can use these reports when events are classified as criminal (e.g., identity theft, credit card fraud, investment fraud, and phony eServices) [17].

The SOCaaS framework consists of nine modules which are described in the following sections.

i. System Agent (SA)

The system agent (SA) is a virtual application installed in-line with cloud services and/or a hardware appliance placed in front of or behind a physical server, network component, i.e., firewall, IDS/IPS, identity management, routers and switches, and storage controllers. The SA is responsible for monitoring and capturing logs (e.g., system logs, application logs, user profile and activities, security logs, and directory service logs), and sends them in real time to the system event management (SEM) module.

The SA can perform certain changes to the security device as a response to an event. Therefore, the SA must have system level privileges to manage the security devices and applications. The SA is flexible in the sense that it can be configured to filter unwanted traffic or processes. However, it is light in the sense that it has no impact on the performance and availability of the cloud security devices.

ii. System Agent Manager (SAM)

The system agent manager (SAM) is responsible for the deployment, maintenance, and discharge of SA agents in the cloud infrastructure and software. It also manages SA agent configuration settings and monitors the connectivity between an SA and SEM.

iii. System Event Managment (SEM)

The system event management (SEM) collects, correlates, and analyzes events and logs from the security devices, system and applications, and respond accordingly. The SEM has the following components:

- *Events and Logs Database (ELD):*

  The events and logs database (ELD) acts as a repository for all events and logs sent by the system agents. It is updated in real time and has a mirrored ELD backup as a contingency in case of failure.

  Events are categorized (e.g. based on defined rules), and stored in a suitable format based on a unified taxonomy. This allows analysts to easily retrieve and group events based on their category.
- *Event Correlation (EC):*

  The event correlation (EC) module is a key system component as it is used to detect events not previously noticed. It uses the information stored in the ELD to derive meaningful results. The correlation results are evaluated against an event knowledge base (EKB) to identify relationships and detect threats. For example, an event in the ELD that a cloud user attempted to log into a cloud web server more than five times could correspond to a 'brute force' login attack in EKB.
- *Event Knowledge Base (EKB):*

  The event knowledge base (EKB) is an online threat knowledge base for cloud providers and the customer infrastructure, platforms and software services. It preserves data from previous known and zero day events. The EKB is shared globally among cloud providers, antivirus vendors, and research institutions to maintain the highest level of cloud security. It contains symptoms that match certain event(s) along with the recommended countermeasures and/or responses.
- *Event Analysis (EA):*

  The event analysis (EA) module allows security analysts to perform advanced research on events. Some events need further explanation and investigation to provide additional details. Other events require long periods of time (e.g., days or weeks) before launching an attack. Therefore, advanced analysis and correlation functions can be employed to understand the source and motivation of certain event.

iv. Event Response (ER)

The event response (ER) module provides appropriate responses according to predefined rules. Typically, requests are sent automatically to the SAs to configure the cloud devices according to the recommend countermeasures. In the case of an event that needs in depth analysis, an analyst will determine the response the first time, and add this action as a response for similar events in the future.

v. Integration Agent (IA)

The integration agent (IA) ensures the operational compatibility of any legacy cloud security devices with SOCaaS system. Any security system, device, or application not integrated with the SOCaaS system does not participate in the event generation, detection, and analysis process. In fact, this can pose a threat to cloud services since any attack or compromise to that device or system will virtually be undetected. Thus, it is essential that the integration agent be used during the development process and prior to cloud customer platform migration to the cloud.

vi. Compliance and Audit Checking (CAC)

Discussion

The compliance and audit checking (CAC) module regularly checks for compliance with security policies to ensure they are enforced and operational. The CAC continuously scans all security devices and reports any events deemed to be non-compliant with regulatory requirements and customer SLA agreements. For example, if a cloud customer is hosting an online payments system, it must ensure the cloud provider complies with payment card industry data security standards (PCI-DSS) [18].

vii. Security Assessment (SAss)

The security assessment (SAss) module determines what risks are inherent to which cloud assets. As part of the security assessment, vulnerability and stress assessments are conducted regularly on every cloud system or service to determine its survivability against any a malicious event. This process is done for both existing cloud services and services under development. The SAss is an automated periodic assessor. It ensures that the necessary cloud security controls are adequately integrated into each cloud service of every customer as per SLA and regulatory requirements.

viii. Physical Security Monitoring (PSM)

The physical security monitoring (PSM) module enables cloud customers to monitor their critical or sensitive information processing facilities. It enables the SOCaaS system and cloud customers to measure the readiness of the facility to an emergency event (i.e., electrical failure, communication failure, temperature and ventilation failure, fire, and floods), as per recovery requirements. The PSM is connected to the physical access controls and sensors such as motion detectors to document unauthorized individuals entering a facility.

ix. Reporting

Reporting is integrated into every SOCaaS module given above. All event reports are aggregated to the central reporting module. The correlation of these reports provides a representation of all phases of the events. It also provides event summaries with forecasts to assist management personnel in making informed decisions on future projects.

Cloud customers and service providers can be granted access to the reporting module based on contractual agreements. Law enforcement authorities can also access reports and forensic analysis if criminal activity has occurred.

Every connection between the SOCaaS system and a service provider domain is encrypted using encryption keys of a suitable length. For instance, events sent from an SA to the ELD are encrypted using a virtual private network (VPN), i.e., point to point tunnelling protocol (PPTP) and IP Security (IPSec) protocol configuration. The Traffic between the SOCaaS system and a cloud provider must be protected against unauthorized interception and attacks such as a man-in-the-middle attack which can result in the systems being compromised.

6. DISCUSSION

In this section, we discuss the advantages of the proposed SOCaaS framework and how it achieves the objectives identified in Section 4.

The proposed framework improves the ability of a cloud organization to rapidly detect, analyse, and respond to malicious events. It can also assist in ensuring cloud providers and customer cloud security event management and meet regulatory compliance requirements. This system also provides information which can aid in making informed decisions on future software, applications, and infrastructure development.

The SOCaaS system can be operated by a trusted third party to manage cloud provider security devices and appliances. The trusted SOCaaS party will possess the best practices in operating and supporting different security operation centre platforms. This provides the security assurance and transparency demanded by cloud customers. Delegating a third party to monitor and manage cloud provider security systems encourages cloud providers to increase investment in service functionality and security [19]. The SOCaaS entity operating as a business interest will invest in well trained security personnel and adopt established SOC operational and analytic procedures. These procedures will be aligned with cloud provider's and customer's business requirements. It should also establish an organizational relationship and have regular meetings with cloud service providers and customers. This facilitates productive discussions and information sharing which can aid in updating service level agreements and regulatory compliance requirements. It can also support customer software development and vulnerability assessment.

The proposed framework combines people (i.e., SOC managers, security engineers, event analysts, and security system and device administrators), SOC platforms (i.e., event management technology), processes and procedures to provide event monitoring, detection, correlation, and response to all cloud

security events. Physical surveillance is also incorporated. An important advantage of SOCaaS is that it can detect malicious events that a single information security application or one layer of security devices may fail to recognize. Monitoring of all cloud services and processes through the collection of cloud security system events and logs enables efficient and effective event analysis and response on a 24/7 basis.

The approach presented in this paper complements existing cloud security systems. Different from existing solutions, the proposed SOCaaS framework is the first to employ a multilayer security model in order that fits with the cloud multi-tangency model, i.e., the fundamental architectural aspect of cloud computing services. It incorporates all security devices in the cloud provider domain. The integration agent ensures security devices are compatible with the SOCaaS SEM module. All cloud security systems (i.e., physical and virtual security devices and applications), participate as the main sources of data for the SOCaaS system, thus ensuring cloud data assurance.

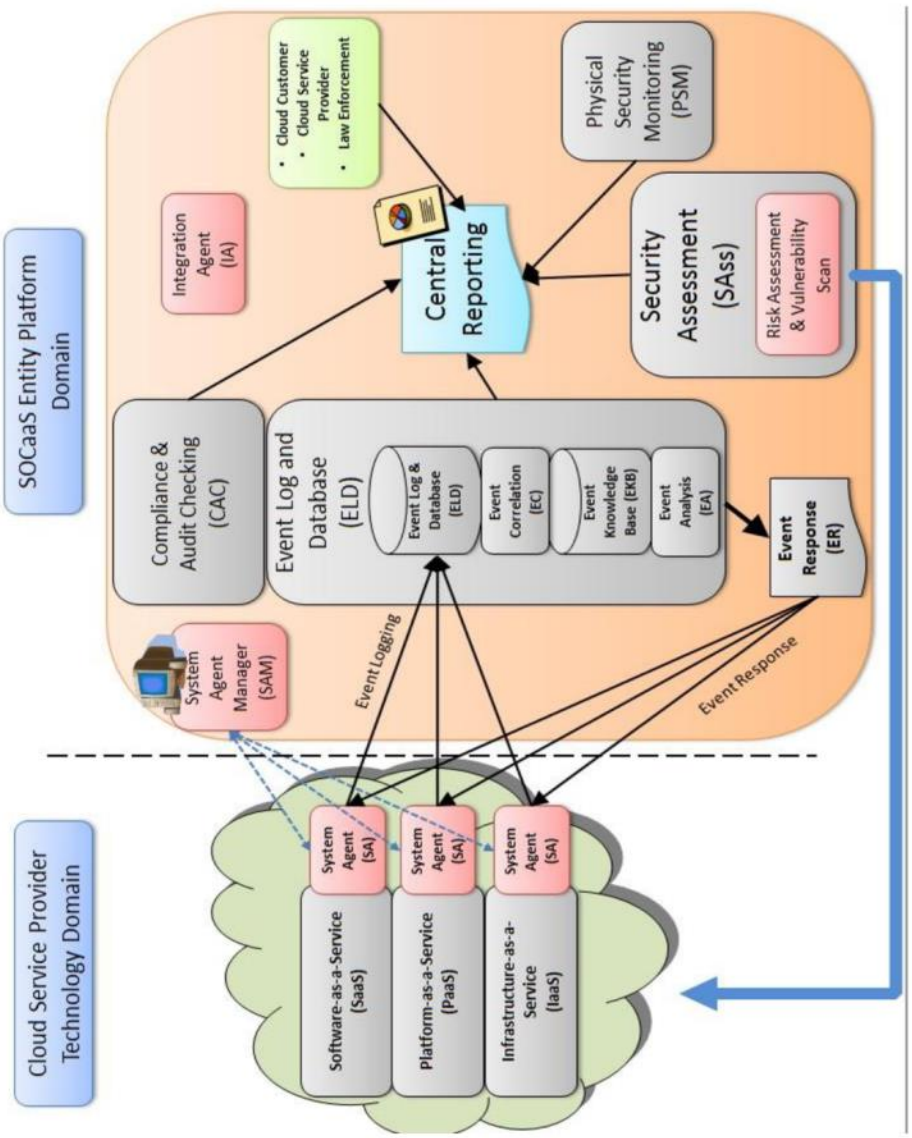


Figure 3 The System Operations Center as a Service (SOCaaS) system architecture.

7. CONCLUSION

Adopting proper cloud security information and event management (SIEM) is essential to the success of cloud service providers' and customers' information assurance. The number and sophistication of malicious events will surely increase. Therefore, it is critical that information security practitioners and researchers contribute to solving cloud information security and privacy issues [20-22].

The proposed SOCaaS framework is based on a multi-layer security model which fits the architectural complexities of a cloud environment. This framework enables trusted entities to establish a security operation centre (SOC) to monitor and manage cloud service provider security appliances, applications, and software. In accordance with cloud customer SLA, policies and regulatory requirements, the SOCaaS framework provides security assurance for critical and sensitive cloud services. It is based on the correlation of events collected from security devices with an event and threat intelligence database. This correlation along with advanced event analysis and forensics assists in detecting and protecting against threats to the cloud systems. The ongoing risk assessment to cloud assets ensures security controls are in place to withstand any external or internal threats. Detailed reporting and event summaries with are delivered to all personnel, including management, to aid in making informed decisions.

The Federal Risk and Authorization Management Program (FedRAMP) recently proposed legislation to force cloud service providers to undergo third party assessment organization (3PAO) evaluation. This is required to meet the minimal security requirements outlined by the Federal Information Security Management Act (FISMA) [23-26]. This legislation will encourage cloud service providers to invest in a secure and reliable cloud infrastructure. We predict that organizations providing security assessment and security operations will be established in the near future. The proposed framework will increase customer confidence and trust in adopting cloud services as it will reduce losses (of data, monetary, and reputation), and increase the return on information security investment (protecting cloud services against known threats and unforeseen events).

REFERENCES

[1] J. Meszaros, "Towards security management in the cloud utilizing SECaaS," *Proceedings WSEAS International Conference on Cloud Computing*, Austria, November 2012.

[2] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0," *Cloud Security Alliance*, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011.

[3] S. Hiroyuki, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," *IEEE/IPSJ International Symposium on Applications and the Internet*, pp. 121-124, 2010.

[4] Symantec Corporation Technical Report "State of Enterprise Security," *Symantec Corporation*, http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf, 2010.

[5] PWC, "Global State of Information Security Survey," *Price Waterhouse Coopers (PwC)*, http://www.pwc.com/es_CO/co/publicaciones/assets/global-state-of-information-security-survey-2011.pdf, 2011.

[6] Cloud Industry Forum, "Cloud UK: Adoption and Trends," *Cloud Industry Forum*, http://www.cloudindustryforum.org/downloads/whitepapers/cif-white-paper-1-2011-cloud-uk-adoption-and-trends.pdf, 2011.

[7] F. F. Alruwaili and T.A. Gulliver, "CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services," *International Journal of Latest Trends in Computing*, Vol. 4, No. 4, pp. 151-158, December 2013.

[8] T. Finne, "A conceptual framework for information security management," *Elsevier Computers & Security*, Vol. 17, pp. 303–307, 1998.

[9] D.W. Straub, "Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment," *Dissertation, Indiana University Graduate School of Business*, 1986.

[10] Security as a Service Working Group, "Defined categories of services 2011 version 1.0," *Cloud Security Alliance*, https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_7_SIEM_Implementation_Guidance.pdf, October 2011.

[11] A. Blumstein, J. Cohen, & D. Nagin, "Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates," Assembly of Behavioural and Social Sciences (US). *National Academy of Sciences Panel on Research on Deterrent and Incapacitative Effects*, Washington DC, pp. 431, 1978.

[12] T. Probst, E. Alata, M. Kaaniche, V. Nicomette, & Y. Deswarte, "An Approach for Security Evaluation and Analysis in Cloud Computing," *Safecomp*, France, September 2013.

[13] B. Niekerk, & P. Jacobs, "Cloud-based security mechanisms for critical information infrastructure protection," *IEEE International Conference on in Adaptive Science and Technology*, pp. 1-4, November 2013.

[14] R. Marty, "Cloud application logging for forensics," *ACM Symposium on Applied Computing*, pp. 178-184, March 2011.

[15] M. Hussain, & H. Abdulsalam, "SECaaS: security as a service for cloud-based applications," *ACM Conference on e-Services and e-Systems*, Kuwait, April 2011.

[16] R. Montesino, S. Fenz, & W. Baluja, "SIEM-based framework for security controls automation," *Information Management & Computer Security*, Vol. 20, No. 4, pp. 248-263. 2012.
[17] E. Casey, "Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet," *Elsevier Inc, Academic press*, 2011.
[18] Payment Card Industry (PCI), "Data Security Standard - Requirements and Security Assessment Procedures," *Payment Cards Industry Security Standards Council*, Version 1.2.1., July 2009.
[19] S. Hiroyuki, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," *IEEE/IPSJ International Symposium on Applications and the Internet*, pp. 121-124, 2010.
[20] P.S. Pawar, M. Rajarajan, S. Krishnan Nair, and A. Zisman, "Trust model for optimized cloud service," *Springer Trust Management VI IFIP Advances in Information and Communication Technology*, Berlin, Vol. 374, pp. 97-112, 2012.
[21] M.L. Kaufman, "Can public-cloud security meet its unique challenges?," *IEEE Security and Privacy,* Vol. 8, No. 4, pp. 55-57, 2010.
[22] "Top Threats to Cloud Computing. March 2010," *Cloud Security Alliance*, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Last viewed (10-04-2014).
[23] "Third Party Assessors (3PAO)," *The Federal Risk and Authorization Management Program (FedRAMP),* http://cloud.cio.gov/fedramp/3pao, Last viewed (04-04-2014).
[24] M. Kozlovszky, M. Trocsik, T. Schubert, and V. Póserné, "IaaS type cloud infrastructure assessment and monitoring," *IEEE International Convention on Information and Communication Technology Electronics and Microelectronics*, pp. 249-252, 2013.
[25] "Information Security," *Federal Information Security Management Act (FISMA),* http://csrc.nist.gov/drivers/documents/FISMA-final.pdf. Last viewed (15-03-2014).
[26] D.E. Issa, "Federal Information Security Amendments Act of 2013'" *Library of Congress*, http://thomas.loc.gov/cgi-bin/bdquery/z?d113:h.r.1163:/. Last viewed (01-02-2014).

BIOGRAPHY OF AUTHORS

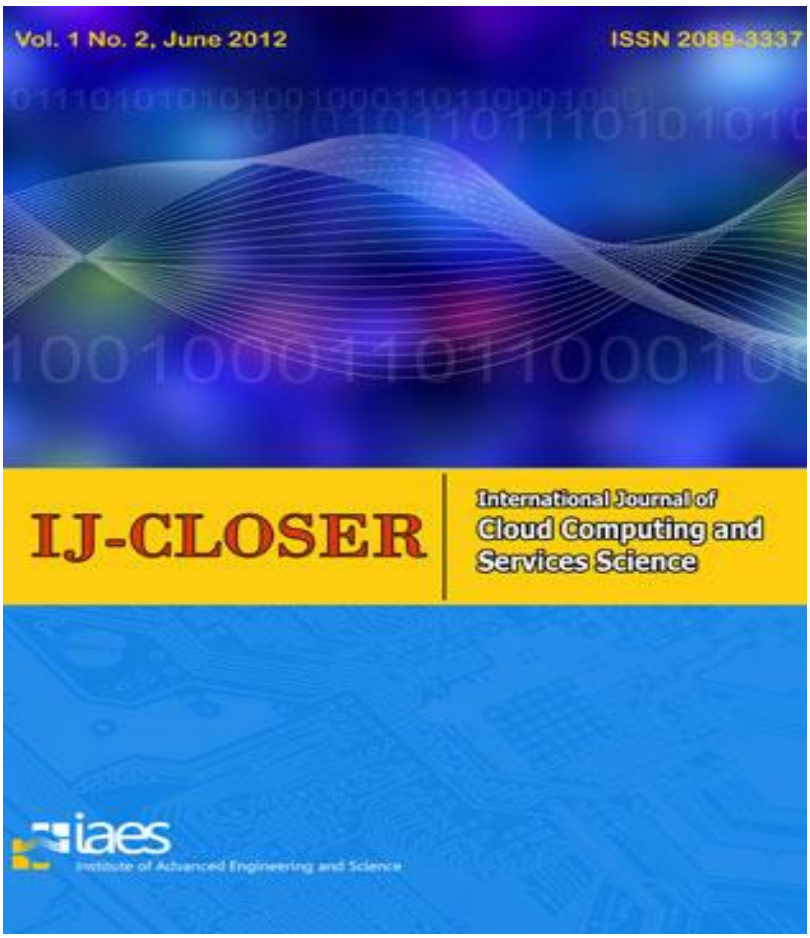
Fahad F. Alruwaili is a faculty member at computer science department at University of Shaqra, Saudi Arabia. He works as information security and computer networks consultant with over nine years of practical and administrative experience. He earned his BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he achieved his MS degree in Computer, Information, and Network Security with first class honour from DePaul University, Chicago USA. In 2011, he received his first class honour in his second MS in Information Systems and Technology from Claremont Graduate University, Los Angeles USA. He is currently working on his Ph.D. degree in University of Victoria, the Department of Electrical and Computer Engineering, Canada. He has research interests in technical and theoretical views of cloud security and privacy.

T. Aaron Gulliver received the Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.

Chapter 5

SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services

As published in *International Journal of Cloud Computing and Services Science*, August 2014



This article appeared in Vol. 3, Issue. 4, published by *International Journal of Cloud Computing and Services Science Copyrighted to © 2012 IAES Institute of Advanced Engineering. The attached* copy is furnished to the author for internal non-commercial research and education use, including for instructions of the authors institution and sharing with colleagues.
Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.
In most cases authors are permitted to post their version of the article to their personal websites or institutional repository. http://www.iaesjournal.com/

iaes Institute of Advanced Engineering and Science

International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.3, No.4, August 2014, pp. 189~198
ISSN: 2089-3337

SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services

Fahad F. Alruwaili, T. Aaron Gulliver
Department of Electrical and Computer Engineering, University of Victoria

Article Info

Article history:

Received Jun 19th, 2014
Accepted Jul 26th, 2014

Keyword:

Service Level Agreement (SLA), Security Operations Center (SOC), Compliance, Monitoring, Trust, Privacy, Cloud Services

ABSTRACT

Cloud customers migrate to cloud services to reduce the operational costs of information technology (IT) and increase organization efficiency. However, ensuring cloud security is very challenging. As a consequence, cloud service providers find it difficult to persuade customers to acquire their services due to security concerns. In terms of outsourcing applications, software, and/or infrastructure services to the cloud, customers are concerned about the availability, integrity, privacy, and legality of the hosted service. In this paper, a secure service level agreement (SecSLA) framework is proposed to alleviate these concerns and provide security control assurance to cloud customers. The framework is proactive in detecting violations of SecSLA parameters based on a cloud security operations center as a service (SOCaaS). In addition, a trusted third party can use this framework to audit and monitor SecSLA compliance.

Copyright © 2014 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Fahad F. Alruwaili
Department of Electrical and Computer Engineering
University of Victoria, PO Box 1700, STN CSC
Victoria, BC V8W 2Y2, Canada
Email: fruwaili@uvic.ca

1. INTRODUCTION

Cloud computing services have been the subject of significant recent interest among computing practitioners and researchers. These services are delivered on demand and on a pay-as-you-use basis. Cloud computing is one of the most substantial changes in the history of the information technology (IT) industry. This is because it promises to provide improved functionality, flexibility, and scalability through the delivery of virtualized computing resources. In addition to the agility in providing these resources, cloud customers can reduce costs by acquiring these virtualized resources instead of traditional internal IT resources [1]. Cloud computing services are delivered over the internet and provide scalable processing power and storage [2]. The three main models of delivering these services are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [3].

The major hindrance to the adoption of cloud services has been concerns with regards to security, compliance and information privacy. According to a recent survey by Gartner Inc. [4], a leading information technology research and advisory company, the most sought after cloud security services are email, application, identity, and access management protection. They predict that the market for cloud security services will reach USD 3.1 billion by 2015. The key to providing security assurance to cloud customers is the contractual agreements with cloud service providers. A service level agreement (SLA) is a contract between legal entities that describes the services expected by cloud customers, the quality of service (QoS), payments for compliance, and penalties in the case of SLA violations [5]. Current SLAs for cloud computing services are typically limited to service availability, performance requirements, and penalties for violations, and thus do not adequately address cloud information security and data privacy issues.

The absence of comprehensive security controls combined with the lack of methods and standards to implement them makes it very difficult for cloud service providers to provide trustworthy virtualized services [6]. This paper presents a secure service level agreement (SecSLA) framework for cloud service environments to address this problem. We previously developed security operations center as a service (SOCaaS) [7] to monitor cloud services and its compliance with customer requirements. The SOCaaS system enables trusted third party entities to manage cloud service provider security appliances, applications, and software to efficiently and effectively detect, analyse, and respond to malicious cloud events. The SOCaaS system does not only collect and analyze events and logs from every security device, but also correlates these logs to identify relationships and proactively detect threats. This improves the response time and accuracy of incident detection. The system event management (SEM) component in the SOCaaS system is utilized in the design of the SecSLA framework. The SEM allows cloud customers to transparently monitor control compliance with their SecSLA parameters and detect violations.

In this paper, the proposed SecSLA framework consists of multiple components including a security controls matrix, log database, compliance and audit checks, and a console for creating and editing SecSLA control parameters. Activity theory is used as the basis for determining the controls for security compliance, and these controls are detailed in the security controls matrix. This taxonomy matrix is based on security controls recommended by the cloud security alliance (CSA), and combines industry accepted security standards, controls and frameworks such as NIST SP800-53, COBIT, ENISA IAF, HIPAA, ISO 27001/27002, NERC CIP, PCI DSS, and FedRAMP [8].

The remainder of this paper is organized as follows. The next section presents the motivation for this work based on customer requirements. In Section 3, the related literature is discussed, and Section 4 outlines the goals of this paper. Section 5 defines service level agreements and describes the construction of the SecSLA framework. Provisioning and negotiation of the cloud security controls workflow process are also outlined. Section 6 provides a discussion of the framework, and finally some conclusions are given in Section 7.

2. MOTIVATION AND CUSTOMER REQUIREMENTS

Organizations wanting to outsource their IT infrastructure, platforms, and applications to cloud service providers should revise their organizational, legal and operational requirements prior to making any decisions. In addition, organizations must assess and document the sensitivity, value, and criticality of their data and information assets. They should also update and document the risks associated with their critical assets. Without this classification and the associated risk assessment, it is not possible to determine the cloud security service requirements and compliance controls. In addition, this exercise will ensure that the security and privacy requirements of cloud customers are properly defined in their initial request for proposal (RFP) and prior to outsourcing to cloud services. This can later be translated into a SecSLA that defines suitable controls provided by the cloud provider. Each SecSLA parameter corresponds to a control or a set of controls. If the acquired cloud services do not conform to the SecSLA parameters, the cloud customer can either accept the risk associated with a failure to protect the services or transfer to a more secure cloud service provider.

3. RELATED WORK

In traditional IT settings, domain specific security controls such as those recommended by the National Institute of Standards and Technology NIST-800-53 standard [9] can be applied. However, new components outside traditional information systems (e.g., cloud computing services) were not designed to be protected by these security controls and policies and therefore are considered insecure [10]. Chaves et al. [11] explored the existing state of security in cloud SLAs. Their survey results indicated the need for improved SLA security specifications and a framework for monitoring and managing secure SLA agreements. This paper addresses these concerns by provides a cloud-specific security controls table and a SecSLA monitoring framework, as well as a control provisioning process.

Bernsmed et al. [6] suggested a monitoring framework for SecSLA through modified web service (WS) agreements. These agreements address security specifications in grid computing and web services, but lack details with regard to cloud security controls, proactive monitoring, and the negotiation process for security controls provisioning. Clark et al. [5] introduced SLA monitoring based on modifications to WS agreements to add the necessary terms and condition to the SLA. Their framework allows trusted third parties to monitor the system and detect SLA violations. However, this approach does not provide security and privacy controls for cloud or traditional IT environments. Further, it cannot be applied to cloud service models (i.e., IaaS, PaaS, SaaS).

In 2003, Keller and Ludwig [12] proposed a web service level agreement (WSLA) framework for specifying and monitoring web enabled service agreements. However, it is not applicable to cloud services and cannot detect security compliance violations. Alhamad et al. [1] proposed a conceptual SLA framework for cloud computing. They defined an SLA framework based on non-functional requirements (e.g., availability, scalability, and response time). While they consider the technical requirements in IaaS, PaaS, and SaaS, the security controls and policy requirements to protect cloud services are not addressed.
In the existing literature on cloud computing services, there is no approach which provides cloud customers comprehensive cloud security and privacy with compliance monitoring and reporting. Given the increasing demand for security and privacy in cloud services and the need to he compliant with regulatory requirements [4], it is very important to implement a suitable framework. The SecSLA framework presented here addresses this problem.

4. OBJECTIVES

The aim of this paper is to develop a secure service level agreement (SecSLA) framework for cloud computing environments. The SecSLA is based on a set of cloud security and privacy controls recommended by the CSA [8]. These controls are defined in a security controls matrix which is presented in Section 5.3. The approach in [7] is used to collect event logs generated by cloud devices and systems. These logs are analysed and the results compared with the SecSLA parameters to ensure compliance and facilitate enforcement. The system can provide cloud customers with both periodic and on demand reports. In addition, customers can add and modify control to provide robust and agile response to changes in security requirements. To achieve this, a control provisioning and negotiation process is provided to facilitate interaction between cloud customers and service providers. The corresponding workflow process is presented in Section 5.4.

It is assumed that cloud service providers will allow not only customers, but also trusted third party agents, to check compliance with SecSLA parameters. These agents are typically hired by cloud customers when they lack the necessary monitoring and auditing capabilities (e.g., auditing experts and auditing systems). In addition, hiring a professional third party promotes accuracy, transparency, and compliance with SecSLAs.

5. THE SECURE SERVICE LEVEL AGREEMENT (SecSLA)

This section provides the SLA and SecSLA definitions, as well as the theory used to develop the SecSLA cloud security controls matrix. The SecSLA control negotiation and provisioning workflow process is also presented as well as the system for monitoring and enforcing the SecSLA.

5.1. SLA and SecSLA Definitions

An SLA is a contractual document between a cloud customer and a cloud service provider. It describes the required services, service parameters, service guarantees, and the actions required in case of SLA violations. Typically these actions include the penalties service providers have to pay to their customers if the SLA parameters (e.g., service performance metrics), are not satisfied [1], [13]. Conversely, the SecSLA specifies security and privacy control policies. It describes the availability, confidentiality, integrity, and privacy parameters and the associated controls needed to protect cloud services. While the SecSLA can be a component of the SLA, it is a separate document. In this paper, a controls matrix, control provisioning and negotiation workflow process, and monitoring system are proposed to ensure proper security service levels and compliance and enforcement of SecSLA parameters.

5.2. The SecSLA Concept

The SecSLA framework (shown in Figure 1 and described in detail in Section 5.5), is based on activity theory as introduced by Engestrom [14],[15]. The application of this theory to the objectives in Section 4 provides a basis for determining actions for security noncompliance and violations. It provides means of addressing complex cloud security requirements by allowing technical or non-technical personnel to apply the necessary rules and policies to achieve a given outcome. According to Figure 1, the object (applying security and privacy controls to each SecSLA parameter) is achieved by involving subjects (cloud customers, providers, and auditors) who use tools or mediating artifacts (e.g., SecSLA framework, SOCaaS [7], and event management) to perform the necessary tasks to meet the SecSLA requirements. The tasks are accomplished through a division of labour (e.g., between the cloud provider and compliance auditor). The subject functions within the respective community (i.e., service provider and external parties) through rules (i.e., information security and privacy policies, legal obligations and mandates, organizational goals) to determine the basis for the required set of security and privacy requirements (i.e., SecSLA parameters).

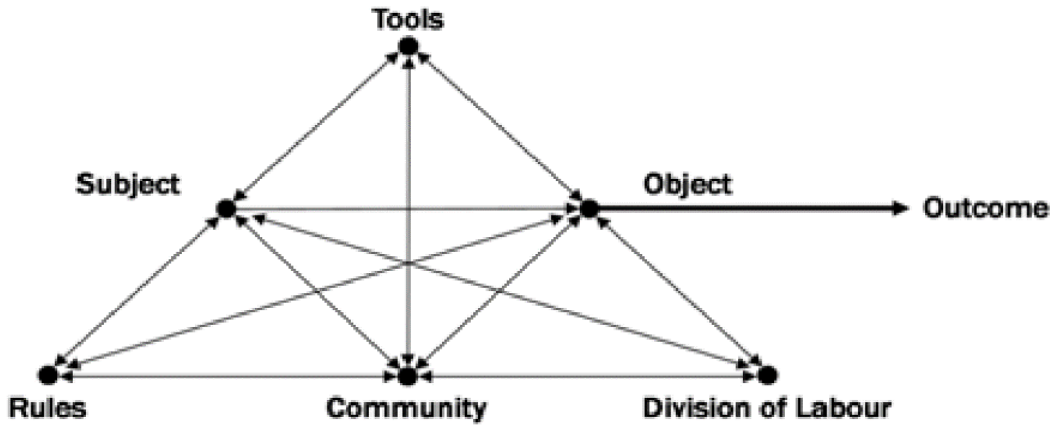


Figure 1. The activity theory system model [15].

5.3. The SecSLA Taxonomy Matrix for Cloud Security and Privacy Controls

The cloud security and privacy controls are identified in this section with respect to four main domains: confidentiality, integrity, availability, and privacy. Table 1 shows the domain, relevant control name, and its application to the cloud service models, i.e., IaaS, PaaS, and SaaS. Note that the service criticality and control priority criteria for a control can vary depending on the customer. Typically, criticality is classified as low, medium or high, and control priority from P0 to P3 (P0 indicates no control, P3 indicates a higher priority than P1 and P2). Therefore, if a cloud service is marked as highly classified, the priority can be set to P3 indicating that a set of security controls must be applied.

Table 1 gives a sample of the most critical cloud security controls. In an actual implementation a longer list would be required. The goal is to provide cloud customers with tailored security controls. If after the SecSLA is defined a new control is required by the cloud customer, negotiations can be conducted with the cloud provider to discuss its feasibility and applicability.

Table 1. The cloud security controls matrix [15].

Control Domain	Control Name	Control Description	Application to Cloud Service Model		
			SaaS	PaaS	IaaS
Privacy	**Data Retention**	The policies and procedures for storing cloud data for compliance and/or other reasons as defined in the SecSLA. The storage location (country) is an important element of the SecSLA.	✓	✓	
Confidentiality	**Data Leakage**	The security mechanisms employed to prevent data leakage. These include the access control policy, user account management/identity management, and access enforcement for cloud assets. For example, a cloud user may require dual authorization (two forms of approval) to access cloud services and/or data.	✓	✓	✓
Privacy and Confidentiality	**Secure Disposal of Data**	The policies and mechanisms for the complete removal of customer data from the cloud without any possible recovery. These may include media sanitization to release cloud provider control media for reuse. If the media cannot be sanitized, then it must be physically destroyed.	✓	✓	

Confidentiality	**Classified Data Protection**	The encryption mechanisms and protocols employed to protect cloud data in storage, processing, and transmission according to the customer SecSLA data classification. The cryptographic module is installed within supervisory engine to protect against data disclosure to another virtual machine (cloud tenant). In the network layer, cloud customer sessions are encrypted to protect against disclosure.	✓	✓	✓
Confidentiality	**Cloud Storage**	The encryption employed by the cloud service providers. Typically they are required to employ strong encryption (e.g., 256 bit AES), but only the data owners (cloud customers) have access to the keys. Therefore, cloud customer must adopt a secure key management system.	✓	✓	
Confidentiality, Availability, Integrity, and Privacy	**Incident & Vulnerability Management**	The intrusion detection and prevention systems implemented in the layers of the cloud model. This prevents cloud services from viruses, cyber-attacks, and other known or zero day attacks. In addition, cloud service providers must perform periodic penetration testing and vulnerability scans to detect system/application weaknesses and take necessary corrective actions (e.g., system patches). Antivirus software is mandatory to protect cloud servers, customers and virtual machines. Service providers must make incident and vulnerability information available to all affected customers.	✓	✓	✓
Confidentiality, Availability, Integrity, and Privacy	**Trusted Third Party Assessment**	The cloud service providers must allow access to external trusted third parties to audit and assess compliance with the SecSLA. This can be both prior to cloud service acquisition and during service operations. All cloud systems are assessed, e.g. physical, procedural, technical, legal, and compliance controls. It can be conducted at planned intervals or on demand as required to maintain SecSLA compliance.	✓	✓	✓
Confidentiality	**Virtualization (Hypervisor) Security**	The cloud service provider must implement isolation controls to shield critical cloud assets and sensitive data from other tenants. Sessions that need stronger controls should be segregated from machines that implement insufficient security controls. In addition, access to the hypervisor must be restricted and strong authentication employed, e.g. two-factor authentication.		✓	✓

5.4. The SecSLA Control Provisioning and Negotiation Process

Security and privacy control request changes can originate from different locations. For example, a cloud customer may call, email, or web request a service provider to add or edit security controls in the SecSLA. The cloud customer can hire a trusted third party cloud agent or an expert to monitor SecSLA compliance. While a cloud customer can choose from an existing security controls matrix, they can also request a new control, which for example can result from a new security or privacy mandate. These requests typically originate from the chief security officer (CSO) and/or chief privacy officer (CPO) or their delegates.

Figure 2 shows the security and privacy control request negotiation workflow. The steps in this process are outlined below.

1. The CSO and/or CPO receive a new regulatory compliance request or an update to a security and/or privacy policy.
2. The cloud security agent (CSA) receives the request, assigns a tracking number, informs the initiator, and forwards the request to the security and privacy control personnel of the cloud service provider. The CSA is an automated service that manages the requests received electronically via emails, online forms, and automated phone answering agents. It assigns the necessary request information (e.g., initiator information and request parameter information), and forwards the request to control personnel for request revision and assessment. This process can also be executed manually if the CSA administrator receives the request in person or via a voice call. The request information is then sent to the control provisioning and negotiation system.
3. The control personnel review the request and assign it to the appropriate control based on the existing controls matrix.

4. The request is forwarded to the cloud operations personnel to check compatibility with the customer cloud services. If there are no issues, the control is applied to the customer services and this is reported back to the cloud agent. The cloud agent updates the SecSLA and informs the customer of the successful change and request completion.
5. If an issue occurs that prevents completing the request, for example when there is a conflict between the SecSLA and the original SLA. For instance, when applying the new security or privacy control, the CPU time and memory usage can be degraded such that it affects the functionality of a cloud service. This must be resolved prior to applying the security control. In this case, the solution may be to increase the allocated CPU time and memory, which will result in additional costs to the customer. Once the issue has been resolved, the control personnel will instruct the cloud security agent to update the SecSLA and inform the CSP/CPO of request completion.

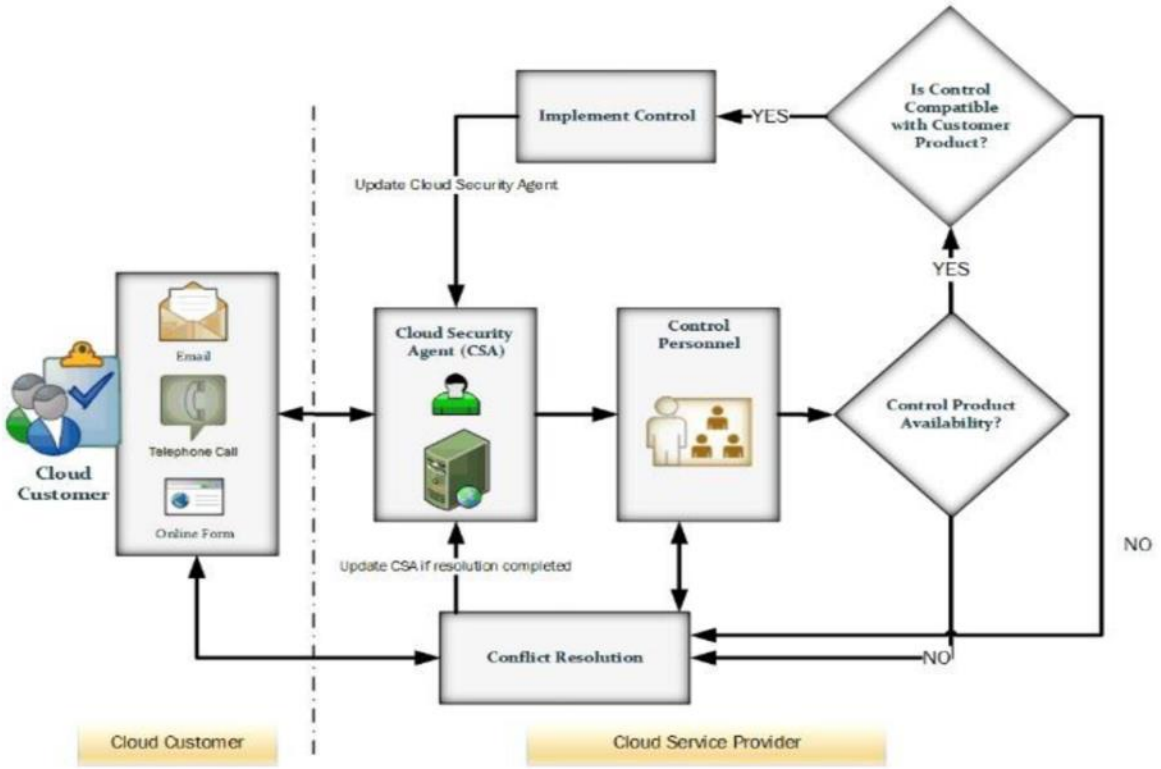


Figure 2. The security and privacy control request negotiation workflow.

5.5. The SecSLA Framework

The SecSLA framework is presented in Figure 3. It is a standalone system to minimize the impact on the performance of virtualized services, yet it interacts with many components of the cloud system. For example, the SecSLA system checks with security devices (e.g., firewalls, antivirus applications, intrusion detection and prevention systems, identity and management and access control systems), to ensure SecSLA polices are enforced.

The framework consists of the following main components:

5.5.1 Log Database (LD)

The LD is responsible for collecting and storing logs from security devices, policy profiles, event management, and the hypervisor in real time. The LD provides a taxonomy for these logs. For example, the LD classifies logs as logs collected:

- *from firewall devices in the IaaS layer*

- *form user activities in the PaaS layer*
- *from virtual machine (VM) sessions*
- *from the event management system*

The LD also reports if it fails to collect from or reach a device to a system administrator or analyst who will assess the cause and take the necessary steps to recover from the failure. The LD as the main repository for logs, it requires online backup in case of failure.

5.5.2 Compliance Monitoring Engine (CME)

The CME continuously checks the LD database for any deviation between the applied security controls and security controls matrix (SCM) parameters. Any deviation triggers a violation to the customer SecSLA. The CME performs advanced analysis to detect security control violations. For example, if a cloud customer requests incident and vulnerability management control to protect their virtual resources, the control is granted and listed as active in their profile. Now, if logs collected from the event management system indicate that this control is not listed as active, a SecSLA violation is triggered. As another example, suppose a customer requests control of secure web service activities. The service provider will perform the following controls and apply them to the customer web service:

 # Disable HTTP – TCP port 80, <egress=1, ingress=1>
 # Disable IITP – UDP port 80, <egress=1, ingress=1>
 # Disable HTTP – TCP 8080, <egress=1, ingress=1>
 # Enable IITPS – TCP port 443, <egress=1, ingress=1>
 # Enable HTTPS – UDP port 443, <egress=1, ingress=1>

If a TCP service request on port 80 is then found to be open or TCP/UDP HTTP connection establishment is acknowledged, a SecSLA violation is triggered.

5.5.3 Security Controls Matrix (SCM)

The SCM provides a control profile for each cloud customer. From Section 5.3, each profile consists of security and privacy parameters for each service. Each parameter corresponds to a security control or a set of security controls in the service provider domain. For example, if a parameter is to provide protection against incidents, the control is to place the customer service under the supervision of the incident and vulnerability management system. As another example, if a customer wants a certain service to be classified as public and highly available, then the corresponding security controls will be set to P0 (no controls) and the availability set to 1 which represents 100% service availability (0.5=50% of the time the service is available). In practice it is hard to achieve 100% availability due to, for example, routine maintenance. However, the five nines (99.999%) is commonly taken to indicate high availability and reliability of computing services.

5.5.4 Cloud Customer Console (CCC)

The CCC enables cloud customers to negotiate SecSLA parameters. The negotiation process was described in Section 5.4.

.

5.5.5 Reporting and Notification

This component provides involved parties (i.e., customers, service providers, and trusted third party compliance auditors), with detailed compliance reports and notification of violations. The report lists the customer SCM parameters and the corresponding controls. It also indicates either compliant or non-compliant for each SecSLA parameter. A justification is given if non-compliance is indicated. Notifications are quickly sent to all involved parties in the form of email and/or text messages if a violation is detected (e.g., customers unable to reach services, customer data unencrypted, an incident that affects customer services is not reported). These reports can be scheduled weekly and also delivered on demand depending on the circumstances. Generating the reports and notifications requires that logs be processed and checked for compliance in real time.

In Figure 3, the left side of the framework consists of the cloud service provider domain which contains security systems, devices, policies, and controls. These work together and exist on each cloud service model (IaaS, PaaS, and SaaS). The logs generated from these systems are examined by the LD for control compliance by checking against the customer profiles in the SCM. It is important for cloud providers

to ensure that all logs are collected by the LD in a timely manner, otherwise false or missed violations may occur which will result in erroneous notifications and reports.

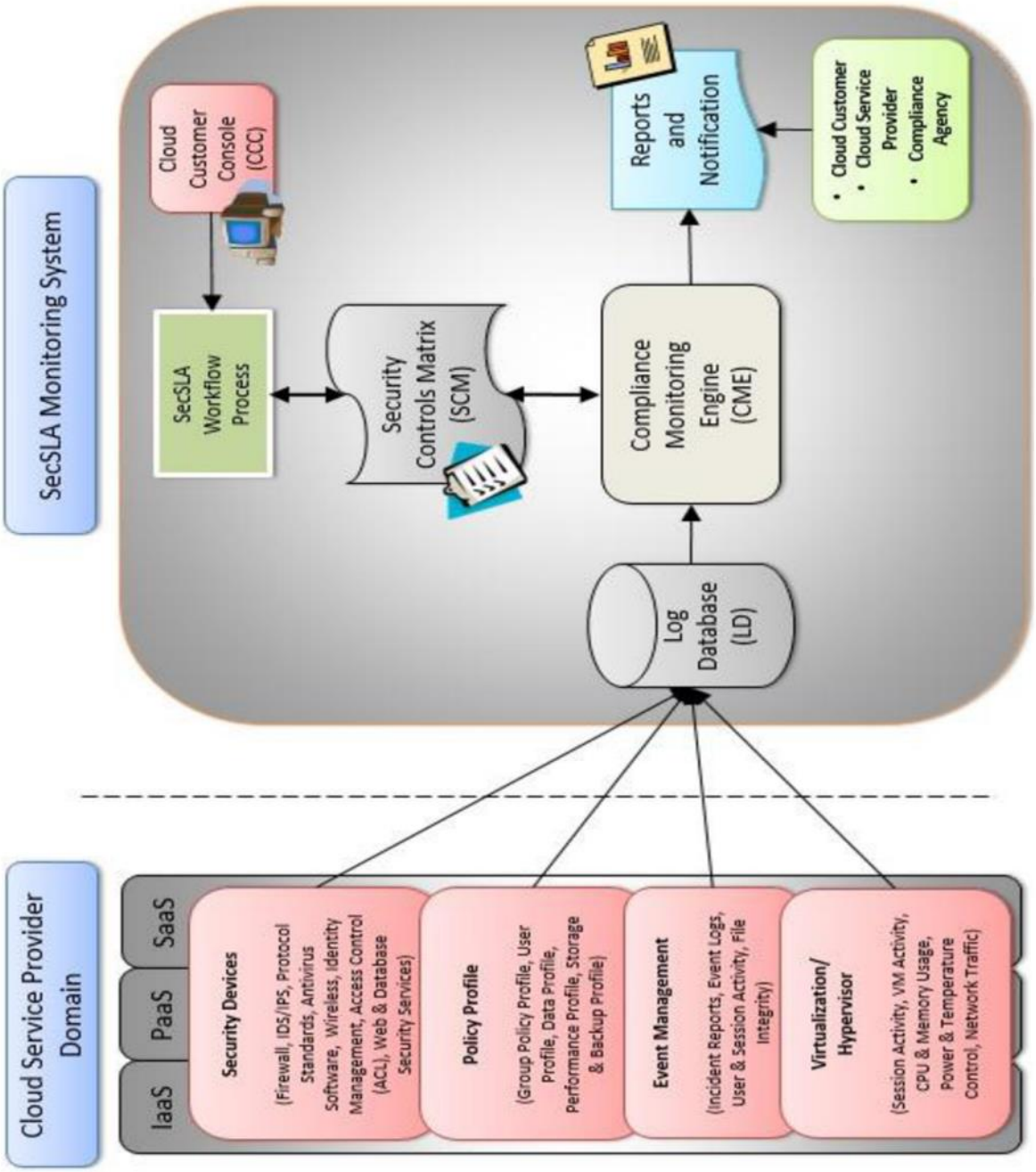


Figure 3. The SecSLA system framework.

6. DISCUSSION

In this section, the advantages of the proposed SecSLA framework are discussed based on the objectives given in Section 4. The SecSLA framework was developed according to cloud security controls recommended by CSA and implemented using a cloud security matrix (CCM Version 3) [8]. While cloud customers receive periodic reports from cloud providers regarding SecSLA compliance, transparency will be greatly improved if cloud customers employ a trusted third party as a compliance agent to monitor and verify that the SecSLA is not violated. Continuous verification and monitoring also increase customer trust and acceptance of cloud services. The monitoring component in the SecSLA framework is an extension of the SOCaaS approach presented in [7] which provides comprehensive security monitoring and event management for cloud services. The SecSLA monitoring system detects any deviations from the agreed upon terms and proactively alerts cloud customers and providers of violations via email and text notifications.

The security and privacy controls are the key component of the SecSLA framework as they alleviates the majority of cloud customer security and privacy concerns. Each control corresponds to a parameter in the SecSLA and these are typically defined in the early stages of the negotiation process. This framework also provides a negotiation system for cloud customers to request, edit, or remove security controls on their cloud services. A conflict resolution process is included for situations where a requested control is not viable or is not listed as an option in the controls table.

The SecSLA is a set of contractual requirements that addresses the four main security concerns, confidentiality, integrity, availability, and privacy of cloud information. Functional and business process requirements are not included since most cloud providers have reached a sufficient level of maturity in these areas. However, security and privacy controls must be improved, which will require significant investment by service providers. The proposed SecSLA framework motivates these investments as it will increase the trust, compliance transparency and enforcement of cloud providers.

7. CONCLUSION

Current cloud service level agreements (SLAs) have parameters for availability, quality of service and penalties for violations, but few are provided for security and privacy [6]. Further, cloud service providers do not offer detailed security and privacy SLA parameters. In addition, there is a shortage of tools for cloud customers to provision, monitor, and enforce security and privacy controls. A recent survey by the European network and information security agency (ENISA) indicates that while SLAs are often used to address service availability, security parameters are poorly covered. Moreover, many cloud customers often do not monitor SLA security on a continuous basis which leaves them unaware of security violations [16], [17]. Section 2 stressed the importance of cloud customers performing a risk assessment and data classification of their information assets prior to outsourcing their assets to the cloud.

In this paper, a new security SLA (SecSLA) framework was proposed to address the shortcomings of current SLAs in terms of cloud confidentiality, integrity, availability and security and privacy controls. The framework components are compliance monitoring of the SecSLA parameters, provisioning and negotiation of cloud security controls, security controls matrix, and reports and notifications. The monitoring system was developed based on a recently proposed approach to collecting, analysing, and responding to events via data logs [7]. The SecSLA framework enables cloud customers and trusted third party auditors to monitor SecSLA compliance and the efficiency and effectiveness of controls on customer services. The main goal of this work is to promote the adoption of cloud services by cloud customers. The proactive control monitoring promotes trust, increases transparency, and emphasizes information security and data privacy controls.

ACKNOWLEDGEMENTS

The research work of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia

REFERENCES

[1] M. Alhamad, T. Dillon, and E. Chang, "Conceptual SLA Framework for Cloud Computing," *IEEE International Conference on Digital Ecosystems and Technologies*, pp. 606-610, April 2010.

[2] E. Badidi, "A Cloud Service Broker for SLA-Based SaaS Provisioning," *IEEE International Conference on Information Society*, pp. 61-66, June 2013.

[3] M. Peter and T. Grance, "The NIST definition of cloud computing (draft)." *NIST special publication (800-145)*, January 2011.

[4] Stamford, and Conn., "Gartner Says Cloud-Based Security Services Market to Reach $2.1 Billion in 2013," *Gartner Inc.*, http://www.gartner.com/newsroom/id/2616115, October 2013.

[5] K. P. Clark, M. E. Warnier, F. M. Brazier, and T. B. Quillinan, "Secure monitoring of service level agreements," *IEEE International Conference on Availability, Reliability, and Security*, pp. 454-461, February 2010.

[6] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim,"Security SLAs for federated cloud services," *IEEE International Conference on Availability, Reliability and Security*, pp. 202-209, August 2011.
[7] F. F. Alruwaili, and T. A. Gulliver, "SOCaaS: Security Operations Center as a Service for Cloud Computing Environments," *submitted for publication on International Journal of Cloud Computing and Services Science*, May 2014.
[8] Cloud Security Alliance Research, "Cloud Controls Matrix v3.0," *Cloud Security Alliance*, https://cloudsecurityalliance.org/research/ccm/, September 2013.
[9] J. T. Force, "Security and Privacy Controls for Federal Information Systems and Organization," *NIST Special Publication (800-53)*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, April 2013.
[10] M. L. Hale, and R. Gamble, "SecAgreement: Advancing Security Risk Calculations in Cloud Services," *In Proceedings of the IEEE World Congress on Services*, pp. 133-140, June 2012.
[11] D. Chaves, S. Aparecida, C. B. Westphall, and F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing," *IEEE International Conference on Networking and Services*, pp. 212-217, March 2010.
[12] A. Keller, and H. Ludwig, "The WSLA Framework: Specifying and Monitoring Service Level Agreements for Web Services," *Journal of Network and Systems Management*, Vol. 11, No. 1, pp. 57-81, March 2003.
[13] Y. Chi, H. J. Moon, H. Hacigümüş, and J. Tatemura, "SLA-tree: a framework for efficiently supporting SLA-based decisions in cloud computing," *International Conference on Extending Database Technology*, pp. 129-140, March 2011.
[14] J. Show, "Information Security in Practice from an Activity-Theoretic Perspective," *In Proceedings of the Annual Security Conference*, pp. 241-248, April 2007.
[15] Y. Engestrom, "Activity Theory and Individual and Social Transformation," *Perspectives on activity theory*, pp. 19-38, 1999.
[16] J. Luna Garcia, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," *In Proceedings of ACM Workshop on Cloud computing security*, pp. 103-112, October 2012.
[17] M. Dekker, and G. Hogben, "Survey and Analysis of Security Parameters in Cloud SLAs Across the European Public Sector," *European Network and Information Security Agency (ENISA)*, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector, December 2011.

BIOGRAPHY OF AUTHORS

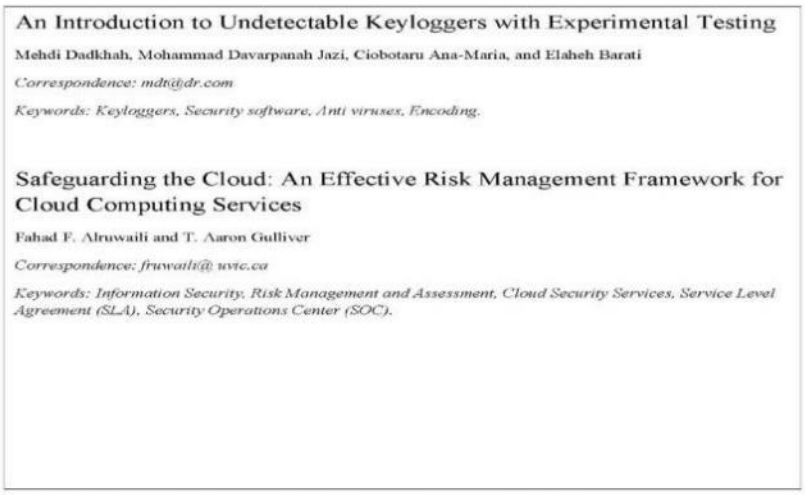
Fahad F. Alruwaili is a faculty member at computer science department at University of Shaqra, Saudi Arabia. He works as information security and computer networks consultant with over nine years of practical experience and research development. He earned his BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he achieved his MS degree in Computer, Information, and Network Security with first class honour from DePaul University, Chicago USA. In 2011, he received his second MS degree in Information Systems and Technology from Claremont Graduate University, Los Angeles USA with first class honour. He is currently working towards achieving Ph.D. degree in University of Victoria, the Department of Electrical and Computer Engineering, Canada. His research interests are in the technical and theoretical views of information security and data privacy.

T. Aaron Gulliver received the Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.

Chapter 6

Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services

As published in *International Journal of Computer Communications and Networks*, September 2014



An Introduction to Undetectable Keyloggers with Experimental Testing

Mehdi Dadkhah, Mohammad Davarpanah Jazi, Ciobotaru Ana-Maria, and Elaheh Barati

Correspondence: mdt@dr.com

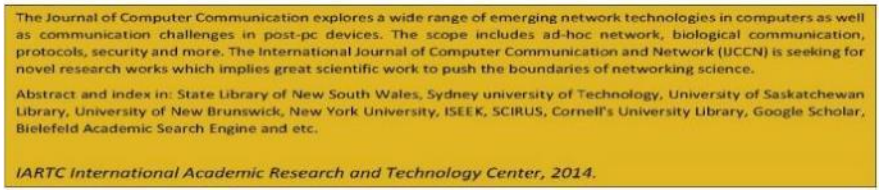
Keywords: Keyloggers, Security software, Anti viruses, Encoding.

Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services

Fahad F. Alruwaili and T. Aaron Gulliver

Correspondence: fruwaili@ uvic.ca

Keywords: Information Security, Risk Management and Assessment, Cloud Security Services, Service Level Agreement (SLA), Security Operations Center (SOC).



This article appeared in Vol. 3, Issue. 3, published by *International Journal of Computer Communications and Networks, Copyrighted to © Galactic Bridge - Research & Technology Publisher, Malaysia*. The attached copy is furnished to the author for internal non-commercial research and education use, including for instructions of the authors institution and sharing with colleagues.
Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.
In most cases authors are permitted to post their version of the article to their personal websites or institutional repository. http://iartc.net/index.php/index

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services

Fahad F. Alruwaili and T. Aaron Gulliver

Abstract—Cloud computing services have attracted the attention of many organizations seeking flexible, simple, and efficient system development, operation, and support. The cost advantages of cloud services motivate the outsourcing of IT systems to the cloud. However, there is a lack of awareness of the security risks associated with cloud services. These risks and the associated threats could jeopardize the success and even the survivability of organizations that adopt cloud services. To address this issue, a risk management framework is proposed in this paper which leverages the previously proposed security operations center as a service (SOCaaS) combined with a secure service level agreement (SecSLA) to provide security requirements and compliance. The framework is self-aware of the organization assets and the associated security risks and vulnerabilities. Automated tools are provided to identify, classify, evaluate, and control the information security and data privacy of cloud systems and services. The proposed framework supports cloud protection by identifying threats and vulnerabilities in cloud systems and recommending steps to ensure their confidentiality, integrity, and availability (CIA).

Index Terms—Information Security, Risk Management and Assessment, Cloud Security Services, Service Level Agreement (SLA), Security Operations Center (SOC).

1 Introduction

CLOUD computing has revolutionized the provisioning of computer systems and services. Organizations can reduce costs, lower energy consumption, and access sophisticated information technology (IT) facilities to meet evolving needs via pay-as-you-go cloud computing service models. The increasing popularity of cloud services has made them a promising alternative for future IT systems [1], [2]. However, the complexity of cloud services and their risk management creates new challenges for organizations. This requires the development of new techniques to provide efficient and reliable security risk management for cloud computing environments [3].

When cloud computing service models were first developed, the focus was primarily on service performance, convenience, on-demand deployment, and functionality. Conversely, information security and risk control were a low priority [4]. This has resulted in a reluctance by potential users to adopt cloud services due to issues regarding cloud service reliability, security, availability, privacy, and security measures within service level agreements (SLAs) [5], [6], [7]. In [8], it was shown that there are significant costs associated with cyber attacks due to lost productivity, revenue and customer trust. Cloud service interruptions are considered one of the most serious risks that cloud service providers and customers face. In February, 2008, Amazon cloud services were down for six hours and their storage (S3) and elastic compute cloud (EC2) services were unavailable for three hours [9]. In early 2009, Google webmail (Gmail) was down for three hours preventing more than 113 million subscribers from accessing their email and document services (Google Docs) [9]. In addition, Microsoft cloud services (i.e., Hotmail, SkyDrive, and Office 365) were unavailable for three hours in September 2011 [10]. Table 1 shows the results of a 2011 survey by the Cloud Industry Forum (CIF) of 450 senior IT and business personnel on cloud adoption and trends [11]. This shows that the top 4 issues in the cloud environment are data security at 64%, data privacy at 62%, and cloud availability and reliability. Therefore, information security and data privacy are considered the greatest challenges facing widespread adoption of cloud computing services [12].

The cloud computing paradigm represents a fundamental transition in how IT services and resources are procured and provided [36]. Many people believe that cloud computing will become far more than a scablable computing platform as new cloud services and models emerge [37], [38]. However, cloud computing is fraught with risks to information security, privacy, and compliance requirements. These risks should be carefully examined before any cloud service is procured [39], [40].

In this paper, a risk management framework is proposed to address the security concerns of cloud service providers and customers. This framework is based on best practices

- *Fahad Alruwaili is a Ph.D. student in the Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 1700 STN CSC Victoria, BC V8W2Y2 Canada. E-mail: fruwaili@ uvic.ca.*
- *T. A. Gulliver is a Professor in the Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 1700 STN CSC Victoria, BC V8W2Y2 Canada. E-mail: agullive@ece.uvic.ca.*
- *The research work of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia*

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

and guidelines developed by the cloud security alliance (CSA) [12] in conjunction with a cloud controls matrix (CCM) [13] to manage cloud security risks and threats. These controls are aligned with industry accepted security standards and guidelines such as NIST SP800-53, COBIT, ENISA IAF, HIPAA, ISO 27001/27002, NERC CIP, PCI DSS, and FedRAMP [13]. The framework utilizes the previously developed security operations center as a service (SOCaaS) [14], [15] to monitor cloud services and its compliance with customer requirements. The SOCaaS system enables trusted third parties to manage cloud service provider security appliances, applications, and software to efficiently and effectively detect, analyse, and respond to security threats and events. The SOCaaS system not only collects and analyses events and logs from all security devices, but also correlates these logs to identify relationships and proactively detect threats. Thus, it improves the response time and accuracy of threat detection. In addition, the framework includes a secure service level agreement (SecSLA) to provide monitoring of security control activities and their compliance with customer requirements which promotes transparent and trusted handling of cloud issues and customer concerns [16]. Security controls are recommended based on the corresponding service level agreement (SLA). The SOCaaS inventory, detection, and monitoring components are included in the proposed framework. The compliance, violation detection, and monitoring components of the SLAs are also incorporated in the risk management framework.

The risk management framework consists of six modules including the risk management system, the asset inventory and monitoring system, risk control and compliance, online threat repository, reports and notifications, and the risk management console. It facilitates identification of cloud assets, their impact, and the associated compliance requirements according to the cloud organization business and security control strategy. The framework output is delivered to the cloud community (customers, vendors, and service providers), so that informed decisions can be made on the level of investment required to achieve appropriate information protection and risk management.

What are your most significant concerns, if any, about the adoption of cloud in your business?

Only asked of respondents who either currently use cloud or will do at some point in the future	Total	No. employees Fewer than 20	20-200	More than 200
Data security	**64%**	62%	61%	68%
Data privacy	**62%**	68%	61%	60%
Dependency upon internet access	**50%**	53%	58%	42%
Confidence in the reliability of the vendors	**38%**	32%	38%	41%
Contract lock-in	**35%**	30%	43%	30%
Cost of change/migration	**32%**	27%	35%	33%
Contractual liability for services if SLA's are missed	**31%**	16%	38%	33%
Confidence in knowing who to choose to supply service	**28%**	27%	29%	28%
Confidence in the vendors business capability	**24%**	16%	25%	26%
Confidence in the clarity of charges (ie will they be cheap on-prem)	**22%**	16%	26%	21%
Lack of business case to need cloud service	**21%**	11%	27%	22%
Base	**323**	73	112	95

Table 1 Cloud Industry Forum Cloud Adoption and Trends Survey 2011 [11]

2 Organization Requirements and Motivation

The rapid adoption of cloud computing services raises serious concerns regarding the risks and threats that can affect cloud information security and data privacy. Moreover, the cloud multi-tenancy architecture and multi-layer service model creates new and complex threats that can have serious consequences for cloud customers. For example, exploiting a vulnerability in the infrastructure as a service (IaaS) could lead to widespread service disruption and system unavailability [17]. Cloud customers must have a cloud risk management process to ensure adequate protection of their hosted information systems and services [18]. Organizations wanting to out-source their software, platform, and/or infrastructure services to the cloud should first review the security and risk management perfor-

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

mance of potential providers. This must include the security controls and incident response program that are employed.

Cloud customers are attracted to the low cost, flexible (extensible and fast IT solutions), accessible (services anywhere and at anytime), and agile (easily add or remove resources as required) cloud services. This has resulted in a rush to adopt these services without proper attention to security issues [10], resulting in critical business processes and sensitive data being vulnerable. Further, there is a lack of formality that prevents the automation of risk management, for example, documents (most often in a natural language) produced from risk process meetings are often not suitable for this purpose [17].

The risk management framework presented here provides an automated security management process for cloud organizations with feedback for early identification of threats, as well as their likelihood (the probability that the threat will be successfully exploited), and steps for mitigation and control. Detailed reports are provided that include the risks affecting cloud systems and services, the risks associated with threats and vulnerabilities, and recommendations to address these risks. These are designed to help cloud organizations make informed decisions with regards to their information security risk assessment and control requirements.

The next section provides a survey of the literature related to cloud service risks and their management, followed by the proposed approach to control risks and threats. Then the key components of the framework are presented, followed by a discussion of risk detection, response, and control.

3 Related Work

Implementing risk management for systems spread across a cloud environment presents a new and difficult challenge. The Cloud Security Alliance (CSA) [19] provides a governance, risk management, and compliance (GRC) stack to assess both private and public cloud services against industry established best practices, standards and critical compliance requirements. In 2011, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published a new version of the ISO 27005 standard which provides guidelines for information security risk management (ISRM) [20]. This document extends the ISO/IEC 27001:2011 standard which presented the requirements to implement information security management systems (ISMS). However, this standard does not provide a cloud-specific risk assessment methodology or structure. Thus, the ISO/IEC 27005:2011 Clause 6-12 recommendations are followed here to provide the steps necessary for proper risk management of cloud assets.

Fito et al. [21] developed an approach to cloud risk management that provides awareness of potential cloud risks in order to align management decisions with business level objectives (BLOs). While their approach addresses the risks associated with BLOs, i.e., maximizing profit, it does not consider risk management in terms of technical risks, threats and vulnerabilities, and security controls are not discussed. In [22], an enterprise risk management system was presented along with its interaction with internal management systems (e.g., business management systems). The integration of risk management with other business management systems is proposed to improve overall enterprise risk management. An integration platform was presented based on cloud computing resources (i.e., low cost, processing speed, and high and convenient resource allocation and utilization), to support information sharing and the integration of business and risk managed systems. The goal is to improve information sharing and integration between platforms for enterprise risk management. However, cloud business and technical risks and a cloud risk management system were not considered.

Abiodum [23] presented a risk management framework for cloud systems operated and managed by a trusted third party. The advantages of cloud computing services are highlighted in terms of the low cost to implement security and privacy measures. However, an actual risk management framework was not developed. In fact, it is stated that formulating and implementing cloud-specific security protocols and frameworks is a significant challenge for researchers and developers. Zhang et al. [12] also presented a risk management framework for cloud service providers. This framework is based on the standard management cycle (Plan, Do, Check, Act) of the ISO/IEC 27001 standard, and the National Institute of Standards and Technology (NIST) management guide for information technology systems. While their approach has some similarities with the proposed framework, it lacks details on important elements such as the cloud risk control matrix, threats and vulnerabilities, proactive detection and response, risk control strategies, secure service level agreement parameters, and the compliance and monitoring process.

Gold [24] conducted a study of the importance of implementing efficient risk management systems in cloud environments. The key elements to achieve this goal were discussed and a checklist of due diligence items for selecting a data security strategy was presented. High level guidelines for risk management (e.g. data inventory and sensitivity determination), were also given.

Lalanne et al. [25] introduced security criteria to enable control management for sensitive information in a company or in its outsourced services, i.e., cloud services. This is an extension of the ISO/IEC 27005:2011 risk management standard to include controls for web services (e.g. cloud services). However, an implementation that ensures complete control over web (and thus cloud), services is not given.

In [17], a risk and service level agreement management framework was presented to improve governance, risk management and compliance (GRC) in cloud computing environments, but a risk management process, structure, or implementation was not given. The contribution is limited to a statement and discussion of the problems and issues surrounding the design of a cloud computing SLA risk management framework.

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

4 Cloud Risk Management Process and Framework

A risk management process is essential to the cost effective implementation of information security and data privacy measures. Government agencies are now taking steps to guard data privacy and prevent security breaches to cloud services [17]. The risk management framework presented in this paper is tailored to improve the GRC process in cloud computing environments.

The European Network and Information Security Agency (ENISA) classifies risks into three categories: organizational, technical, and legal. Organizational risks are those affecting the cloud community organization structure and businesses (e.g. loss of company reputation). Technical risks are those affecting the confidentiality, integrity and availability (CIA) of cloud services and the supporting systems (e.g. resource-sharing isolation issues, failure to detect and respond to malicious incidents, and data leakage). Legal risks are those associated with legal compliance to domestic and global data security and privacy mandates by regulatory organizations. Cloud customers and service providers must be aware of the risks associated with jurisdiction changes and the liabilities and obligations in the case of, for example, loss of data or service interruption [26], [27].

The Cloud Security Alliance (CSA) is a specialized group of practitioners and researchers formed in 2008 to promote the use of best information assurance practices within cloud computing environments and to deliver cloud security education and awareness. They have published extensively on the threats to cloud computing services [28]. However, their threat model does not classify threats and risk according to the ENISA categories, i.e., organizational, technical, and legal.

4.1 Risk Management Process

In this section, the major components of the risk management process are discussed.

4.1.1 Asset Inventory, Evaluation, and Classification

The process of risk identification begins with the creation of an inventory of cloud information assets and an assessment of their value to cloud customers and service providers. The development of an asset inventory is an iterative process that includes cloud information, software, hardware, networking elements, policies and procedures, and people, and assets are classified using these categories. For example, networking elements includes servers, firewalls, proxies, routers, and switches. Software includes applications and operating systems, while people include trusted employees, authorized contractors, and non-trusted organizations.

Cloud assets are evaluated based on their criticality to the success of the corresponding organization using appropriate indicators such as:

- the revenue generated by the asset,
- the cost to replace the asset,
- the cost to protect the asset, and
- the liability if the asset is exposed.

Once this evaluation has been completed, the assets are listed in order of importance. The process of determining the importance of each asset varies within the cloud community. For example, military organizations typically use five data classification levels, top secret, secret, confidential, sensitive but unclassified, and unclassified. Most organizations, however, employ a simpler classification, e.g. public, official use only, sensitive, and classified.

4.1.2 Threat Identification

- *Threat Identification Process*

The threats to cloud customers and service providers are analyzed after identifying and classifying the cloud assets. The focus here is on serious threats so those that are unimportant are ignored. The assessment is based on question such as:

- Does the threat affect business continuity?
- Does the threat affect cloud information assets?
- What is the cost to the cloud customer/provider to recover from a successful threat?
- What is the cost to the cloud customer/provider to prevent a threat occurring?

These questions aid cloud users in developing a framework for threat assessment. The number of questions is determined based on the required details for the threat analysis.

- *Threats to Cloud Services*

There are many threats to cloud computing environments and its security mechanisms. Each threat requires a detailed analysis to assess their potential impact on cloud services [29]. The process of threat identification is an important phase of identifying and assessing cloud risk. Table 2 shows the most important threats to information security and data privacy based on previous studies [30]. The threats have been modified to address cloud risks and provide relevant examples.

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

THREAT TYPE	EXAMPLE
Hardware failure or error	Networking component failure such as a router, firewall, or switch in the cloud infrastructure layer, or an application or storage component failure such as a server or storage controller in the cloud platform layer.
Software failure or error	A firmware failure in the infrastructure or platform operating system, a software error in an application, operating system or firmware, or an outage due to a service interruption.
Quality of service and policy deviation	Failure to apply or monitor security controls to a cloud service, a CPU or memory allocation error, or a compliance violation.
Compromise of intellectual property (IP)	Failure to provide protection against piracy or copyright infringement.
Deliberate software or hardware attack	Software or hardware service outage due to failure to detect and respond to a cyber attack, e.g. virus, worm, distributed denial of service (DDoS) attack, SQL injection, account espionage and unauthorized access, DNS reflection, or a man-in-the-middle (MITM) attack.
Human error or failure	An employee error or a failure to implement a control measure such as two-man control.
Technology obsolescence	A cloud service compatibility issue or an outdated application that poses a potential threat.
Act of nature	Cloud datacenter disruption due to a natural disaster such as a fire, flood, or earthquake. This can also affect the backup sites of a cloud service provider.

Table 2 Important Threats to Information Security and Data Privacy

4.1.3 Vulnerability Identification

Once the cloud assets have been identified, classified and evaluated, the list of vulnerabilities for each asset is reviewed. Vulnerabilities are flaws or weaknesses in cloud assets that could be exploited deliberately or accidently resulting in a security breach, violation of policy, and/or public exposure. This process yields a comprehensive list of cloud assets and their vulnerabilities. Each threat may be mapped to multiple assets, and an asset can have multiple vulnerabilities. The list will likely vary between cloud customers and service providers. This process is somewhat subjective and is based on many factors such as the expertise and knowledge of cloud service personnel.

4.1.4 Risk Assessment

The risk assessment process evaluates the probability that a given cloud vulnerability will be successfully exploited, and the probability of a vulnerability occurring due to a given threat. For instance, if a router in the IaaS layer has a weakness against a denial of service (DOS) attack, then this weakness is the vulnerability, the DOS attack is the threat, and the router is the cloud networking asset. In NIST document SP 800-30 [31], 0.01 denotes a low occurrence and 1.0 a high occurrence (1 to 100 percent). For example, the likelihood that a networking component (e.g. a router), in the IaaS layer can be attacked is calculated based on traffic limits, the authorized load, and event history.

Risk is the probability that a threat will trigger a vulnerability which harms an asset. The risk for a cloud asset is a function of the probability of the vulnerability occurring, the probability of the threat being triggered, and the impact to the organization of a loss of the asset, which can be written as

$$R = f(V, T, A)$$

or less abstractly as

$$Risk = Probability \times Impact$$

To accurately determine risk and the probability of a threat exploiting a vulnerability, the vulnerability history must be examined and future occurrences predicted. Therefore, this probability is not easy to determine and will have some degree of uncertainty since it is partially based on logic and reason. Thus highly trained and experienced risk and information security professionals and auditors must perform this evaluation to obtain reliable probabilities and risk values.

The total risk is obtained using the probability of a threat exploiting a vulnerability and the asset impact assigned and approved by the asset owner. Using the NIST likelihood scale (0.01 to 0.33 = low, 0.34 to 0.66 = medium, 0.67 to 1.00 = high) and impact scale (0.01 to 0.33 = low, 0.34 to 066 = medium, 0.67 to 1.00 = high), if asset A is

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

assigned an occurrence of 0.5 and an impact of 0.7, then the total risk will be 0.5×0.7 = 0.35 or a 35% total risk exposure. Since an organization can never be 100% secure, there will always be a residual risk (RR) equal to the total risk minus the applied countermeasures (residual risk = total risk – applied controls). The next step is to select and apply a control strategy that is appropriate for the cloud customer or service provider risk policy requirements. This is discussed in the next section.

4.2 Risk Control Matrix

The risk control matrix aids cloud customers in making an informed decision on the selection of risk control strategies. This matrix classifies risk controls into four risk control strategies according to the frequency of a threat occurring and its impact as shown in Figure 1 [32]. The four control strategies are discussed below.

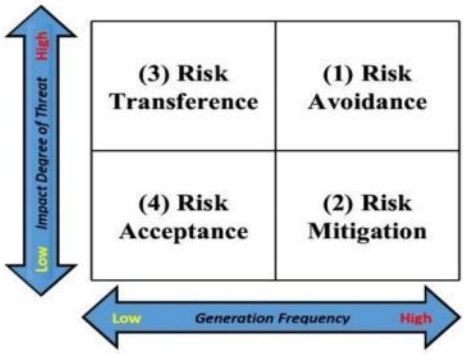


Figure 1 The Risk Control Strategy Matrix [32]

4.2.1 Risk Avoidance

Once the cloud assets have been identified and the associated risks assessed, appropriate countermeasures must be selected to address these risks. The risk avoidance strategy defines the approach taken to prevent exploitation of cloud vulnerabilities (known or perceived). This approach is the preferred control strategy because it can proactively remove detected cloud vulnerabilities and apply protective safeguards/measures. To avoid cloud risks, cloud customers and service providers should:

- Ensure all security control procedures and guidelines stated in the policy are followed, typically by enforcement protocols initiated by management.
- Communicate the policy to all security staff and ensure they have the necessary awareness, skills, and behaviour. Usually this is done as part of employee training and education.
- Implement appropriate information security solutions to eliminate or reduce risks.

For example, consider a vulnerability that affects the login credentials of a cloud user. Once this vulnerability has been detected, the organization should revise the password policy controls to include more advanced security measures and/or techniques (e.g. two-factor authentication). Revision of just the policy is not sufficient as the changes must be communicated to the appropriate personnel so that suitable actions can be taken. The revised password policy is then implemented and monitored. This ensures that the risk avoidance process is followed to avoid risks facing cloud user logins and authentication credentials.

4.2.2 Risk Mitigation

The risk mitigation strategy is a control approach to counter or reduce the impact of exposure of a particular cloud asset. This control is reactive to threats as cloud customers and service providers take immediate action once it is detected. There are several available risk mitigation plans, but the most popular is the incident response plan (IRP). The IRP immediately responds to threats with a predefined or ad hoc set of actions. For instance, if a cloud customer asset is affected by a DDoS attack or virus, the IRP assesses the damage the event has caused and informs the security personnel of the organization in order to develop a coordinated set of actions.

Organizations with sensitive cloud assets should have multiple risk mitigation strategies such as a business continuity plan (BCP) and a disaster recovery plan (DRP). The DRP limits the losses during and after the event. DRP actions usually begin after the disaster and start from the last valid and healthy system recovery point (backup). The BCP ensures the continuation of cloud business activities even if the DRP is unable to completely restore cloud operations. The BCP includes steps to ensure cloud service survivability via a secondary cloud provider as a backup in case the current provider is unable to continue.

4.2.3 Risk Transference

This control strategy is selected if a cloud customer wants to shift the risk to other assets within the service provider facilities, or even another provider. Risk can also be transferred to a third party that has experience in dealing with cloud risks and threats. As an alternative, the risk can be transferred to an insurance company that will undertake the risk for a fee.

4.2.4 Risk Acceptance

This strategy is usually not an acceptable option as it means that the cloud customer or service provider does nothing to protect against vulnerabilities. It is unacceptable for an organization to adopt a security policy to protect employee and customer information but not

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

employ an appropriate risk control strategy. Some organizations choose to accept risks based on the reasoning that they are unlikely to occur, but this is very dangerous. Others understand the risks and accept the impact of threats. In most circumstances, the risks far outweigh the benefits of choosing this approach and thus it is strongly suggested that this risk control strategy be avoided.

4.3 Risk Management Framework

The proposed risk management framework is designed to enable cloud customers and service providers to detect, assess, and monitor the risks and threats to cloud assets. The framework consists of six modules as shown in Figure 2 and described below.

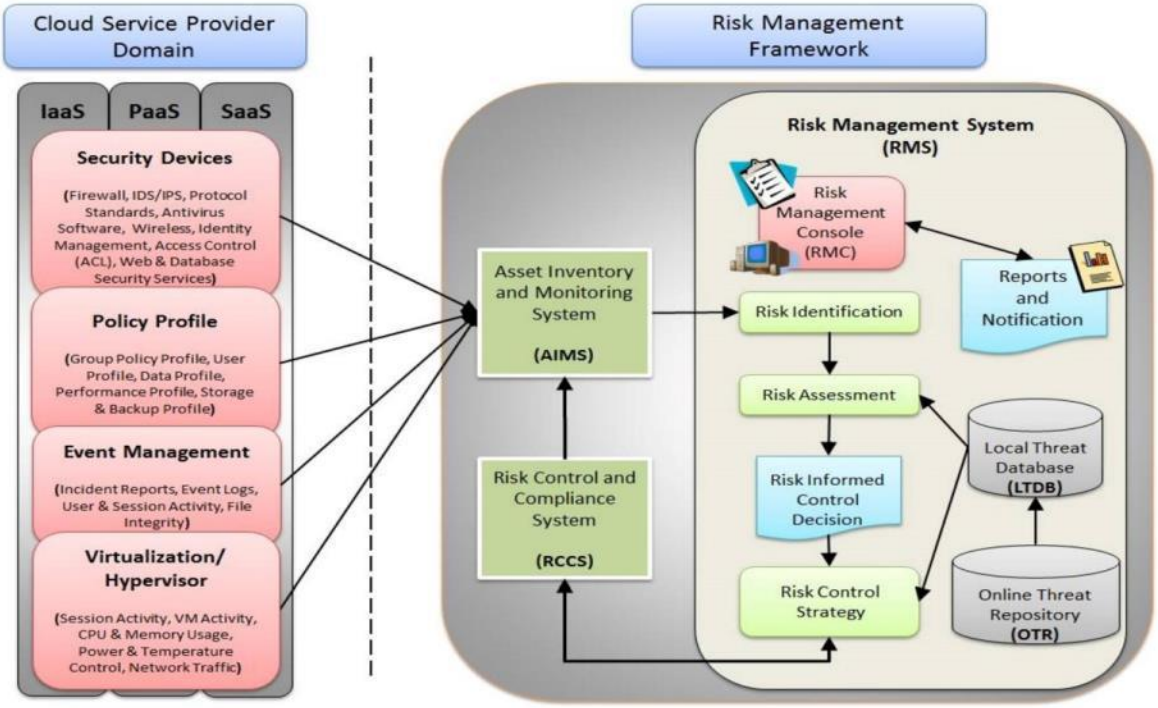


Figure 2 The Cloud Risk Management System

4.3.1 Risk Management System

The Risk Management System (RMS) is the key to achieving effective and efficient cloud risk management. It encompasses the planning, analysis, control, implementation and monitoring of the security risk management strategy. The RMS includes administrative (personnel, policies and procedures) and functional steps for risk identification, assessment, and control. The main components are as follows.

- ***Risk Identification:*** Classify the cloud assets and identify the corresponding risks.
- ***Risk Assessment:*** The risk identification results are used to assess the associated threats and vulnerabilities. Then the likelihood of each threat occurring is determined based on its history and the local threat database (LTDB). The criticality and classification of cloud assets is usually performed by cloud customer personnel (asset owners). Typically, each department within a cloud organization is responsible for assessing the value of the associated assets. They also determine the recovery points according to the recovery time objective (RTO) and the last valid backup point, i.e., recovery point objective (RPO). The RTO and RPO are updated periodically or if an asset changes or is added. Risk assessment should be done regularly (e.g. twice a year or when new assets are deployed). The assessment results are used by

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

security personnel to determine the proper control strategy.

- ***Risk Informed Control Decision***: Key cloud personnel (i.e., cloud business management, system owners, system experts, lawyers and auditors), determine the implementation of risk management and ensure its enforcement via training and a systematic risk methodology. The risk assessment is used to identify assets, their value and classification, threats, vulnerabilities and their likelihood of occurrence. Then a risk-informed decision is made on an appropriate control strategy. The feasibility of the strategy is an important factor in making this decision. Typically, a formal process is employed, e.g. control cost benefit analysis and benchmarking with best practices. The feasibility of a cloud customer or service provider acquiring the control solution and its associated hardware and software infrastructure is also considered.
- ***Risk Control Strategy:*** Once the control decision has been reached, this module ensures the proper implementation of risk controls. It operates in conjunction with the Risk Control and Compliance System (RCCS) to implement and ensure compliance with risk control policies and procedures.

4.3.2 Asset Inventory and Monitoring System

The Asset Inventory and Monitoring System (AIMS) consists of the functional steps discussed in Section 3.1. It detects the assets deployed in the cloud infrastructure, platform, and software layers. The system is responsible for forwarding this information to the RMS for assessing relevant risks, threats, and vulnerabilities. The SOCaaS developed in [14] is employed in the AIMS module due to its detailed analysis and monitoring capabilities for cloud security. The event logs module in the SOCaaS is able to detect and monitor all cloud assets and their supporting technology (hardware and software). The SOCaaS is designed around the threat prevention system CCIPS [15] to enable collaborative detection, analysis, and response to cloud threats. The CCIPS is a threat prevention system based on advanced and cooperative threat knowledge and employs a behavioural database to assist in monitoring and early detection of risks affecting cloud services.

4.3.3 Risk Control and Compliance System

The Risk Control and Compliance System (RCCS) implements and monitors cloud risk controls to ensure compliance with customer service level agreements (SLAs) and with the chosen risk control strategy. It continuously checks if the controls are implemented appropriately and reports any deviations to the reports and notifications module. The RCCS has the capability to check compliance with risk control avoidance (Section 3.2.1) and mitigation (Section 3.2.2) strategies. If cloud customers or service providers employ the risk transference strategy (Section 3.2.3), then the organization undertaking the risks (e.g. insurance company), should enable the RCCS to implement, monitor, and assess the security controls. The risk acceptance control strategy (Section 3.2.4) is not within the RCCS responsibility. The RCCS also updates the risk control strategy document when changes are indicated in the monitoring results. This creates a proper lifecycle and ensures an up-to-date control strategy document. If the monitoring results are below expectations, the RCCS updates the reports and notifications module for further action. Typically, in this case the risk assessment process is restarted to ensure an appropriate risk control strategy is chosen.

4.3.4 Online Threat Repository

The Online Threat Repository (OTR) is a global online threat database that gathers and correlates real-time security threat information from cloud vendors and service providers. It complements the local threat database (LTDB) with comprehensive coverage of cloud threats across cloud customers and service providers. Researchers worldwide also contribute to the OTR. This ensures a high level of security and an effective risk management strategy.

4.3.5 Reports and Notifications

This module provides involved parties (i.e., customers, service providers and trusted third parties), with detailed risk management reports. These reports include the following elements for each cloud asset:

- Risk description
- Risk rating (low, medium or high)
- Threat impact rating (insignificant, minor, moderate, major or significant)
- Vulnerability likelihood (low, medium or high)
- Defined owner, risk owner, and shared responsibilities
- Current risk control description including type of action, control due date and status
- Risk and policy compliance status, i.e., in progress, compliant, or noncompliant
- Control strategy and/or SLA agreement violations
- New and emerging threats
- Periodic risk management activities and evaluation results including previous risk prevention performance and proposed improvements

These reports aid in developing awareness and understanding of current and perceived cloud computing risks and provide a formal structure for reporting these risks. It also provides transparency and promotes accountability for the delivery of appropriate risk controls. As a re-

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

sult, cloud customer trust in service providers is increased and concerns regarding risks are alleviated.

4.3.6 Risk Management Console

The Risk Management Console (RMC) allows risk auditors to access the risk management system continuously to review risk performance, risk control effectiveness, current and new asset identification and classification, and risk control actions. To provide a competitive advantage in risk management performance over competing systems, the RMC enables cloud service providers to obtain detailed current and archived records from the reports and notification module to perform strategic analysis. If these records do not contain the latest risk information, the RMC can initiate the risk identification, analysis, and assessment process by the RMS.

4.3.7 Summary

As shown on the right side of Figure 2, the framework represents an interactive risk management process. The left side shows the cloud service provider domain including the customer and service provider virtual and physical assets (e.g. security systems, devices, policies and controls). The information generated from these systems is shared with the AIMS for asset detection and monitoring. For effective risk management, it is important that service providers ensure all cloud assets are identified and monitored by AIMS and evaluated by the RMS in a timely manner. In addition, providers should report assets that are not detected by the risk management system due to technological barriers (e.g. system incompatibility or obsolescence and hardcopy assets such as policy documents).

5 Discussion

In this section, the advantages of the proposed risk management framework are discussed. It is also shown that the cloud organization requirements identified in Section 2 are satisfied.

Prior to engaging in a partnership with a cloud service provider, a prospective customer should request the necessary documentation to perform a comprehensive review of the provider risk management system and their information security and data privacy program. The proposed framework increases the ability of cloud organizations to rapidly detect, analyse, and respond to threats. The framework risk assessment process is based on a cooperative local and online threat repository database which allows cloud organizations to make informed decisions on risk control strategies.

The proposed risk management framework is based on industry best practices and leverages existing research results. It also incorporates our previously developed cloud information security approaches [14], [15], [16]. The cloud device monitoring proposed in [14] is extended to provide risk management and monitoring of assets. In addition, the cloud threat detection and prevention component in [15] is integrated into the risk identification, assessment, and control (i.e., risk management process), of the framework. The security and threat risk control matrix and recommended measures in [16] for secure service level agreements are employed in the risk control and compliance component of the proposed framework. This allows the risk management system to improve security coverage of cloud services and assets through a risk assessment of threats and vulnerabilities.

The risk management system can be operated by a trusted third party to monitor and analyse sensitive assets of service providers and cloud customers. This trusted third party must employ best practices risk management methodologies and standards to assess the security risks to cloud services. This not only provides robust assessment of cloud threats, but also the transparent and trusted evaluations expected by cloud customers. Delegating a third party to implement and operate the framework will encourage cloud service providers to increase investment in information security research and development [33].

In terms of policy enforcement, the proposed framework engages all cloud organizations in risk management via a top-down approach to monitor the performance of the risk control strategy that has been implemented. This requires that the strategy be communicated to all associated personnel through a training and awareness program. The result is an effective and successful risk management plan with a formal risk methodology and systematic procedures. These procedures are based on the selection of approved risk control strategies that conform to the business requirements of service providers and cloud customers.

An important advantage of the proposed framework is the capability to cooperate with local and online threat management systems to provide comprehensive and detailed risk assessment results. These results are studied carefully by risk assessors and auditors to determine appropriate and feasible control strategies. Collaboration between organizations and risk experts enables the framework to establish proactive risk controls for early detection and assessment of threats to cloud assets.

The approach presented in this paper complements existing cloud security management systems. However, different from existing solutions, the proposed risk management system is the first to employ multilayer security, i.e., risk management framework deployment in the IaaS, PaaS, and SaaS cloud layers, via the utilization of SOCaaS. The use of SOCaaS in [14] fits the cloud multi-tenancy model, which is the fundamental architecture of cloud computing services, because it adopts the principle of multilayer security enabling the addition of security measures in all layers. It incorporates our previous approaches to cloud protection that require the participation of all cloud security systems and nodes, i.e., physical and virtual security devices and applications, in the proposed risk management framework system to ensure all assets are identified and their risks and threats accurately analysed and appropriately controlled.

The proposed framework allows cloud service providers to perform risk assessment and security evaluation of current and prospective cloud customer services. The application and selection of a control strategy is based on the risk

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTG.NET

tolerance of an organization, which is their willingness to accept risk. In addition, cloud customers can examine and evaluate the information security program of their service provider. The proposed risk management framework is a business enabler because it assesses cloud security services to support business initiatives. In other words, it provides flexible security services that are applicable to Infrastructure as a Service (Iaas), Platform as a Service (PaaS), and Software as a Service (SaaS) cloud service models. This ensures the overall efficiency, security and continuity of cloud operations.

6 Conclusion

The number and complexity of malicious threats to cloud systems is increasing. Therefore, implementing an effective cloud risk management system is essential to the success and protection of cloud services. To achieve this goal, information security practitioners and researchers must all contribute in solving cloud risks and threats [28], [34], [35]. Recently, the Cloud Security Alliance (CSA) released version 3.0 of its cloud controls matrix (CCM) that contains a number of baseline controls adjusted to fit cloud computing services and mapped to industry standards, regulations and frameworks by NIST, PCI DSS, HIPAA, COBIT and others [13]. It is strongly advised that cloud organizations review these when selecting risk management controls.

The proposed risk management framework is based on an in depth security model which incorporates the complexities of cloud service layers. It enables trusted entities to conduct risk identification, risk assessment, and risk control for cloud customers and service providers. Risk control is implemented in accordance with cloud customer SLA, policy and regulatory requirements. The framework provides risk assurance for critical and sensitive cloud services by assisting cloud organizations in making risk-informed control decisions. Threat management is based on the correlation of local and online threat management systems that cooperate and correlate new threats among different cloud provider platforms. The iterative risk assessment of cloud assets ensures security controls are in place to withstand external and/or internal threats and prevent asset exposure. Detailed reporting to key personnel is provided to improve the efficacy and efficiency of the risk management lifecycle.

The proposed framework assesses threats such as those presented in Table 2 and recommends measures to control the associated risks (typically via risk avoidance and/or mitigation strategies). The framework performs advanced analysis on security threats, and provides advice to organizations on preventative measures that can be taken to avoid catastrophic incidents via control and recovery strategies. In addition, periodic reports provide cloud service providers with evidence that efforts have been made, i.e., practicing due care and due diligence, to comply with information security and data privacy requirements to protect them from potential litigation and/or prosecution.

References

[1] C. K. Fan, C. M. Chiang, and T. L. Kao, "Risk Management Strategies for the Use of Cloud Computing," *International Journal of Computer Network and Information Security*, Vol. 4, No. 12, pp. 50-58, November 2012.

[2] M. Dou El Kefel, and B. Mohamed, "Risk Management in Cloud Computing," *IEEE International Conference on Innovative Computing Technology*, pp. 127-131, London, UK, August 2013.

[3] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0," *Cloud Security Alliance*, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011.

[4] H. Sato, A. Kanai, and S. Tanimoto, "A Cloud Trust Model in a Security Aware Cloud," *IEEE/IPSJ International Symposium on Applications and the Internet*, pp. 121-124, Seoul, Korea, July 2010.

[5] N. A, Sultan, "Reaching for the Cloud: How SMEs Can Manage," *International Journal of Information Management*, Vol. 31, No. 3, pp. 272-278, June 2011.

[6] N. Stinchcombe, "Cloud Computing in the Spotlight," *Infosecurity Magazine*, http://www.infosecurity-magazine.com/view/4755/cloud-computing-in-the-spotlight/, October 2009.

[7] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," *Proceedings of the ACM Workshop on Cloud Computing Security*, pp. 85-90, Chicago, IL, November 2009.

[8] Symantec Corporation, "State of Enterprise Security Report 2010," http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf, 2010.

[9] C. K. Fan, and T.-C. Chen, "The Risk Management Strategy of Applying Cloud Computing," *International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 9, pp. 18-27, September 2012.

[10] J. R. Kalyvas, M. R. Overly, and M. A. Karlyn, "Cloud Computing: A Practical Framework for Managing Cloud Computing Risk—Part I," *Intellectual Property and Technology Law Journal*, Vol. 25, No. 4, pp. 7-18, March 2013.

[11] Cloud Industry Forum, "Cloud UK: Adoption and Trends for 2011," http://www.cloudindustryforum.org/downloads/whitepapers/cif-white-paper-1-2011-cloud-uk-adoption-and-trends.pdf, 2011.

[12] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments," *IEEE International Conference on Computer and Information Technology*, pp. 1328-1334, Bradford, UK, June-July 2010.

[13] Cloud Security Alliance Research, "Cloud Controls Matrix v3.0," https://cloudsecurityalliance.org/research/ccm/, September 2013.

[14] F. F. Alruwaili, and T. A. Gulliver, "SOCaaS: Security Operations Center as a Service for Cloud Computing Environments," *International Journal of Cloud Computing and Services Science*, Vol. 3, No. 2, pp. 87-96, April 2014.

[15] F. F. Alruwaili and T. A. Gulliver, "CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services," *International Journal of Latest Trends in Computing*, Vol. 4, No. 4, pp. 151-158, December 2013.

[16] F. F. Alruwaili and T. A. Gulliver, "SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services," *International Journal of Cloud Computing and Services Science*, submitted July 2014.

[17] J. Morin, J. Aubert, and B. Gateau, "Towards Cloud Computing SLA Risk Management: Issues and Challenges," *IEEE International Conference on System Science*, pp. 5509-5514, Maui, HI, January 2012.

[18] A. van Cleeff, "A Risk Management Process for Consumers: The Next Step in Information Security," *ACM Workshop on New Security Paradigms*, pp. 107-114, September 2010.

[19] Cloud Security Alliance, "Governance, Risk Management and Compliance (GRC) Stack," http://www.cloudsecurityalliance.org/grcstack.html, March 2013.

[20] International Organization for Staandardization, ISO/IEC 27005:2011, "Information Technology-Security Techniques-Information Security Risk Management," http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56742, 2011.

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Volume 1, Issue 2, September 2014, ISSN 2289-3369
WWW.IARTC.NET

[21] J. O. Fitó, M. Macías, and J. Guitart, "Towards Business-driven Risk Management for Cloud Computing," *IEEE International Conference on Network and Service Management*, pp. 238-241, Niagara Falls, ON, October 2010.

[22] G.-R. Li, H. Liu, and C.-H. Li, "Proposal of Cloud Computing Platform for Enterprise Comprehensive Risk Management," *Information Technology Journal*, Vol. 12, No. 18, pp. 3843-3848, December 2013.

[23] A. S. Abiodun, "A Framework for Implementation of Risk Management System in Third Party Managed Cloud," *Journal of IT and Economic Development*, Vol. 4, No. 2, pp. 19-30, October 2013.

[24] J. Gold, "Protection in the Cloud: Risk Management and Insurance for Cloud Computing," *Journal of Internet Law*, Vol. 15, No. 12, pp. 24-28, June 2012.

[25] V. Lalanne, M. Munier, and A. Gabillon, "Information Security Risk Management in a World of Services," *IEEE International Conference on Social Computing*, pp. 586-593, Alexandria, VA, September 2013.

[26] European Network and Information Security Agency (ENISA), "Cloud Computing: Benefits, Risks and Recommendations for Information Security," https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment, November 2009.

[27] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing," *ACM International Conference on Intelligent Semantic Web-services and Applications*, pp. 1-6, Amman, Jordan, April 2011.

[28] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0," https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010.

[29] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," *IEEE International Conference on Cloud Computing*, pp. 109-116, Bangalore, India, September 2009.

[30] M. E. Whitman, "Enemy at the Gate: Threats to Information Security," *Communications of the ACM*, Vol. 46, No. 8, pp. 91-95, August 2003.

[31] National Institute of Standards and Technology, "Risk Management Guide for Information Technology Systems," *NIST Special Publication 800-30*, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, July 2002.

[32] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, "Risk Management on the Security Problem in Cloud Computing," *ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*, pp. 147-152, Jeju Island, Korea, May 2011.

[33] S. Hiroyuki, A. Kanai, and S. Tanimoto, "A Cloud Trust Model in a Security Aware Cloud," *IEEE/IPSJ International Symposium on Applications and the Internet*, pp. 121-124, Seoul, Korea, July 2010.

[34] P. S. Pawar, M. Rajarajan, S. K. Nair, and A. Zisman, "Trust Model for Optimized Cloud Service," *Trust Management VI, IFIP Advances in Information and Communication Technology*, Vol. 374, pp. 97-112, Surat, India, May 2012.

[35] M. L. Kaufman, "Can Public-cloud Security Meet its Unique Challenges?," *IEEE Security and Privacy*, Vol. 8, No. 4, pp. 55-57, July-August 2010.

[36] A. Baldwin, D. Pym, and S. Shiu, "Enterprise Information Risk Management: Dealing with Cloud Computing," *Privacy and Security for Cloud Computing*, Springer, pp. 257-291, 2013.

[37] A. Baldwin, D. Pym, M. Sadler, S. Shiu, "Information Stewardship in Cloud Ecosystems: Towards Models, Economics and Delivery," *IEEE International Conference on Cloud Computing Technology and Science*, pp. 784-791, Athens, Greece, November-December 2011.

[38] D. Pym, M. Sadler, S. Shiu, and M. C. Mont, "Information Stewardship in the Cloud: A Model-based Approach," *International Conference on Cloud Comp*, Guilin, China, October 2010.

[39] N. Brender and I. Markov, "Risk Perception and Risk Management in Cloud Computing: Results from a Case Study of Swiss Companies," *International Journal of Information Management*, Vol. 33, No. 5, pp. 726-733, May 2013.

[40] S. Srinivasan, "Risk Management in the Cloud and Cloud Outages," in *Security, Trust and Regulatory Aspects of Cloud Computing in Business Environments*, IGI Global, 2014.

BIOGRAPHY OF AUTHORS

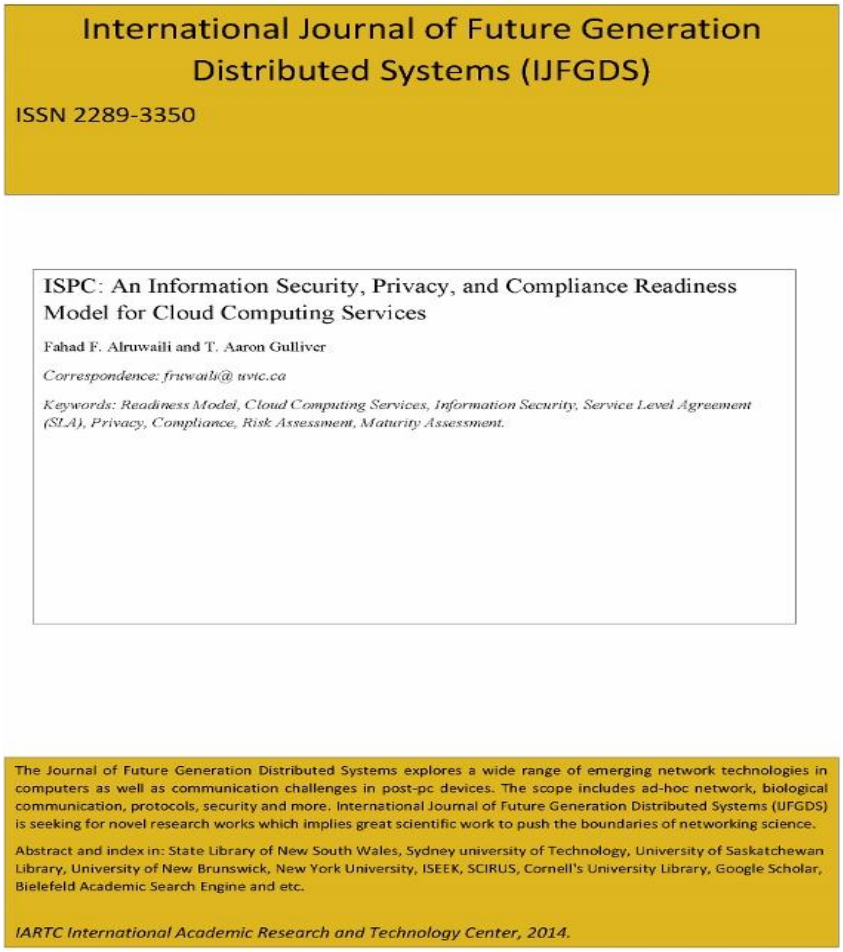
Fahad F. Alruwaili is a member of the Department of Computer Science of the University of Shaqra, Saudi Arabia. He works as an information security and computer networks consultant with over twelve years of practical experience and research development. He earned his BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he rceived the MS degree in Computer, Information, and Network Security with first class honours from DePaul University, Chicago USA. In 2011, he received the MS degree in Information Systems and Technology from Claremont Graduate University, Los Angeles USA with first class honours. He is currently working towards the PhD degree at the University of Victoria, Victoria. BC, Canada. His research interests include the technical and theoretical aspects of information security and data privacy.

T. Aaron Gulliver received the PhD degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.

Chapter 7

ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services

As published in *International Journal of Future Generation Distributed Systems*, December 2014



International Journal of Future Generation Distributed Systems (IJFGDS)

ISSN 2289-3350

ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services

Fahad F. Alruwaili and T. Aaron Gulliver

Correspondence: fruwaili@ uvic.ca

Keywords: Readiness Model, Cloud Computing Services, Information Security, Service Level Agreement (SLA), Privacy, Compliance, Risk Assessment, Maturity Assessment.

The Journal of Future Generation Distributed Systems explores a wide range of emerging network technologies in computers as well as communication challenges in post-pc devices. The scope includes ad-hoc network, biological communication, protocols, security and more. International Journal of Future Generation Distributed Systems (IJFGDS) is seeking for novel research works which implies great scientific work to push the boundaries of networking science.

Abstract and index in: State Library of New South Wales, Sydney university of Technology, University of Saskatchewan Library, University of New Brunswick, New York University, ISEEK, SCIRUS, Cornell's University Library, Google Scholar, Bielefeld Academic Search Engine and etc.

IARTC International Academic Research and Technology Center, 2014.

This article appeared in Vol. 4, Issue. 4, published by *International Journal of Future Generation Distributed Systems, Copyrighted to © Galactic Bridge - Research & Technology Publisher, Malaysia*. The attached copy is furnished to the author for internal non-commercial research and education use, including for instructions of the authors institution and sharing with colleagues. Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.
In most cases authors are permitted to post their version of the article to their personal websites or institutional repository. http://iartc.net/index.php/index

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services

Fahad F. Alruwaili and T. Aaron Gulliver

Abstract—Cloud computing services and their delivery model enable cloud customers to obtain convenient, on-demand provisioning of configurable information technology (IT) resources with minimal investment. Organizations seeking to dramatically reduce costs, increase the speed of software testing and development, and gain agility in adapting to changes are motivated to adopt this new approach to IT services based on a pay-as-you-use model. However, cloud-specific information security, privacy, and compliance (ISPC) risks are a serious concern when migrating to the cloud. In addition, a comprehensive methodology is lacking for assessing the readiness of cloud information security, privacy, and compliance programs. Therefore, we propose an ISPC readiness model for evaluating the readiness of an organization to effectively and efficiently counter cloud threats and address compliance violations. This model includes guidelines and tools to support ISPC readiness evaluation and optimization when migrating to or employing cloud computing services. It also incorporates our prior work on risk assessment of cloud assets via the systems security engineering capability maturity model (SSE-CMM).

Index Terms—Readiness Model, Cloud Computing Services, Information Security, Service Level Agreement (SLA), Privacy, Compliance, Risk Assessment, Maturity Assessment.

1 Introduction

THE cloud computing paradigm presents a transition from computing as a product to computing as a service [1]. The cost-effective cloud service model enables organizations to obtain rapid provisioning of information technology (IT) resources with much less effort. However, the limited information security readiness of cloud computing environments is commonly cited as the greatest barrier preventing organizations from migrating to the cloud [2].

Cloud computing as a new technology presents new challenges in regards to information security, privacy, and compliance (ISPC) requirements [3]. These issues arise from the cloud computing paradigm, in particular the multi-tenancy architecture and multi-layer internet-enabled service model, which creates new and complex threats to cloud computing environments [4], [5]. Thus it is essential that organizations implement a comprehensive assessment methodology for cloud computing services to ensure the safety of their information systems.

The Asia Cloud Computing Association (ACCA) was founded to accelerate the adoption of cloud computing in the region. In 2014, their third survey on the cloud readiness index (CRI) was published [6]. This index is based on ten parameters and provides a measure of the cloud computting awareness and readiness in Asian countries [6]. Figure 1 shows the CRI for 2014. It is clear that data privacy and intellectual property (IP) protection are among the major concerns that limit the adoption of cloud services across the region.

In 2011, the World Economic Forum (WEF) explored the future of cloud computing and developed recommendations for actions that governments and industry can take to accelerate the adoptation of cloud technologies [7]. Their report does not offer prescriptive solutions but rather suggests a charter for further engagement among governments, industry, and academia. OF the eight recommendations made, managing cloud risks, developing regulation requirements, and cloud security and trust were highlighted.

The above studies demonstrate that cloud capabilities can be leveraged to deliver secure, trusted, and optimized services. However, due to the lack of service standardization, secure service level agreements, and trust in the cloud, organizations wanting to transfer their information systems to the cloud are reluctant to do so. A detailed migration plan and an evaluation of its feasibility are required. More specifically, organizations in posesssion of data that is subject to information security, privacy, and/or compliance requirements need a comprehensive methodology for assessing ISPC readiness to addresses potential cloud computing threats [8].

- *Fahad Alruwaili and T. Aaron Gulliver are with the Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 1700 STN CSC Victoria, BC V8W 2Y2 Canada. E-mail: {fruwaili,agullive}@uvic.ca.*
- *The research work of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia.*

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

Country & ccTLD	1. Privacy	2. International Connectivity	3. Data Sovereignty	4. Broadband Quality	5. Government Regulatory Env and Usage	6. Power Grid and Green Policy	7. IP Protection	8. Business Sophistication	9. Data Centre Risk	10. Freedom of Information	CRI 2014 SCORE	RANK	CHANGE
Japan JP	9.5	5.5	8.0	9.1	5.0	7.1	8.1	8.2	6.6	9.7	76.8	1	-
New Zealand NZ	8.8	4.6	7.9	7.6	5.6	9.2	8.6	6.8	7.8	9.5	76.3	2	+4
Australia AU	8.8	4.4	7.6	8.0	5.3	7.8	7.6	6.7	9.4	9.6	75.1	3	+4
Singapore SG	6.0	8.2	7.8	8.8	6.1	5.9	8.7	7.3	7.4	8.6	74.8	4	-
Hong Kong HK	6.8	7.7	7.6	9.3	5.1	5.6	8.1	7.5	7.4	9.6	74.7	5	-2
South Korea KR	9.7	5.5	7.2	9.4	5.1	6.6	5.7	6.9	8.6	8.6	73.3	6	-4
Taiwan TW	4.6	6.3	6.8	8.5	5.0	6.7	7.4	7.4	6.9	8.6	68.2	7	-2
Malaysia MY	5.8	5.8	6.7	7.1	5.2	4.9	6.9	7.2	8.5	8.2	66.2	8	-
Thailand TH	4.0	5.0	6.2	8.0	3.7	6.3	4.4	6.3	7.6	7.8	59.3	9	+4
Philippines PH	5.8	5.4	5.9	4.1	3.7	5.5	5.1	6.1	5.5	9.0	56.1	10	+2
China CN	5.9	3.0	4.8	5.9	4.3	4.3	5.6	6.2	6.5	7.0	53.3	11	-1
Indonesia ID	4.4	2.9	6.2	3.1	3.9	5.7	5.6	6.3	6.4	7.9	52.4	12	-1
India IN	4.6	2.3	6.5	3.6	4.1	5.0	5.3	6.3	3.4	7.8	48.8	13	-4
Vietnam VN	3.6	3.2	5.6	4.2	3.8	4.7	4.1	5.3	6.4	7.0	47.8	14	-1

Figure 1 The 2011 World Economic Forum advanced cloud computing report [53].

2 Organization Motivation and Requirements

Cloud computing provides convenient and on-demand access to a pool of configurable IT resources than can easily be provisioned [1]. However, the rapid advance of cloud computing services raises serious concerns regarding the risks and threats affecting cloud information security and data privacy. Moreover, the cloud multi-tenancy architecture and multi-layer service model create new and complex threats that could be devastating to the cloud community i.e., cloud service providers and customers. For example, an exploited vulnerability in the IaaS cloud model could lead to service disruption and system unavailability [4]. Thus there are significant challenges with regards to developing, provisioning, and managing secure cloud resources [9].

Organizations considering the use of cloud services should have their information security, privacy, and compliance readiness evaluated to ensure the safe and proper migration of their information systems. Information security readiness is commonly cited among IT executives as one of the greatest impediments to organizations leveraging cloud services [1]. Therefore, this paper proposes a readiness model for cloud based information security, privacy, and compliance (ISPC). The focus of this model is the assessment of the three main cloud organization assets i.e., people, information, and technology. *People* are responsible for the operation and maintenance of cloud services. The cloud data forms the *information* processed and produced by these services. The cloud *technology* is the supporting platforms that run the required services. These assets must be identified and regularly documented, inventoried, and prioritized. Typically, the provisioning of cloud services cannot be accomplished without a clearly defined mission that supports the strategic objectives of the organization. The proposed readiness model is a multifaceted assessment model designed to achieve the mission and goals of an organization in terms of the ISPC requirements.

The proposed cloud-specific ISPC readiness model evaluates the current cognition, ISPC settings, and intentions of an organization towards improved security measures to protect cloud data. The term "readiness" indicates the degree of preparedness and inclination to use appropriate methodologies and make informed decisions. This model can be used to evaluate people i.e., technicians, administrators, engineers, managers, and non-IT personnel, in terms of their competency and awareness of known and new information security threats. It provides recommendations to improve existing ISPC implementations in order to enhance the level of readiness through the adoption of appropriate protection and security measures. Note that ISPC measures that are too stringent and/or complex may negatively im-

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

pact ISPC readiness. Further, personnel who have not received adequate training to handle the ISPC enhancements and manage the increased demands, or a lack of financial resources to support ISPC readiness improvements, may limit ISPC performance. To address these issues, an ISPC readiness model is developed using a holistic approach to evaluate the overall factors that contribute to the success or failure of an ISPC program.

The proposed ISPC readiness model employs our previously developed risk management framework for cloud assets [10]. This framework allows cloud organizations to assess risks based on the probability of threats occurring and their potential impact on cloud assets. In addition, the implementation of controls is recommended in order to mitigate and proactively respond to existing cloud risks and unagerial perspective such as improved employee and customer satisfaction, opportunities to develop new applications, and reduced operational costs. Understanding these benefits is far from straightforward and thus they introduced a conceptual framework to assist organizations in determining the cost, suitability and impact of adopting cloud services. However, ISPC challenges and readiness evaluation were not addressed.

A major challenge organizations face when migrating services to the cloud is how to adhere to information security and privacy principles [13]. Many security experts believe that organizations hosting their data and application on the internet and/or adopting the cloud model are vulnerable to new threats and cybercrime activities [16].

Kurdi et al. [13] suggested a framework for evaluating

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

provides guidelines for evaluating the readiness of organizations in achieving these objectives. It outlines the steps that should be performed during the phases of an ISPC project lifecycle. The cloud ISPC readiness model components outlined in the following sections provide asset owners, IT managers, and system professionals with cloud visibility, data analysis and decision capabilities. They also allow organizations to conduct a comprehensive, accurate, and accountable readiness assessment. These results can then be used to determine if the readiness level is sufficient.

To gain *visibility*, an organization must collect data relevant to information security, privacy, and compliance requirements in order to:

- Understand the current information security, privacy, and compliance program including documentation policies, incident response and recovery plans, and technology solutions.
- Understand in detail the IaaS, PaaS, and SaaS cloud service models and activities.
- Efficiently execute the migration plan to the cloud.
- Adequately secure, control, and manage cloud resources.

To perform cloud *data analysis*, an organization must create data reports, logs, and events to:

- Understand current threats and risks facing assets.
- Understand cloud behavior i.e., normal and abnormal.
- Evaluate cloud risks i.e., organizational, technical, and legal.
- Detect, investigate, and eliminate anomalies.
- Provide advanced analysis to determine appropriate responses to threats.

To make appropriate *decisions*, organizations need to:

- Review and revise their risk control strategies.
- Implement adequate security solutions based on the chosen risk controls.
- Initiate a risk/threat response plan.
- Regularly update their risk control strategies.
- Monitor control performance and compliance on a continuous basis, e.g. for enforcement and performance purposes.

The proposed ISPC model is designed to help cloud organizations and those considering migration to the cloud to understand their information security, privacy, and compliance readiness and how it can be improved. This model provides for the:

- Analysis of knowledge within an organization of the relevant information security, privacy, and compliance requirements and mandates.
- Assessment of the preparedness of an organization for cloud threats and compliance risks.
- Sharing of knowledge among IT personnel.
- Documentation and revision of information so that it is easy to use, update, share, understand, and access.

The ISPC readiness model consists of five components as depicted in Figure 3 and discussed below. A flowchart detailing the methodology for evaluating the current and desired ISPC readiness is given at the end of the section. Note that this model can be used to both assess current readiness and improve ISPC preparedness.

4.1 Information Security Model (Cubic Model)

A cubic cloud security model is proposed to assist cloud service providers and customers in planning migration to the cloud. It is a mapping tool between security policies, security attributes, and security control requirements. The output is a representation of the cloud areas that must be addressed during the development and implementation of the ISPC migration plan. Figure 2 shows the three-dimensional (cubic) cloud security model. The intersections are used to identify areas of concern. For example, the intersection between cloud technology, data integrity policy, and cloud storage defines the data integrity requirements for ISPC migration and optimization. One security control to address this intersection is the implementation of encryption mechanisms and intrusion detection and prevention systems. This will protect the integrity of cloud data and alert security personnel of any unauthorized modifications to this data. Once an area of missing or weak security measures has been identified, security control recommendations can be proposed.

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

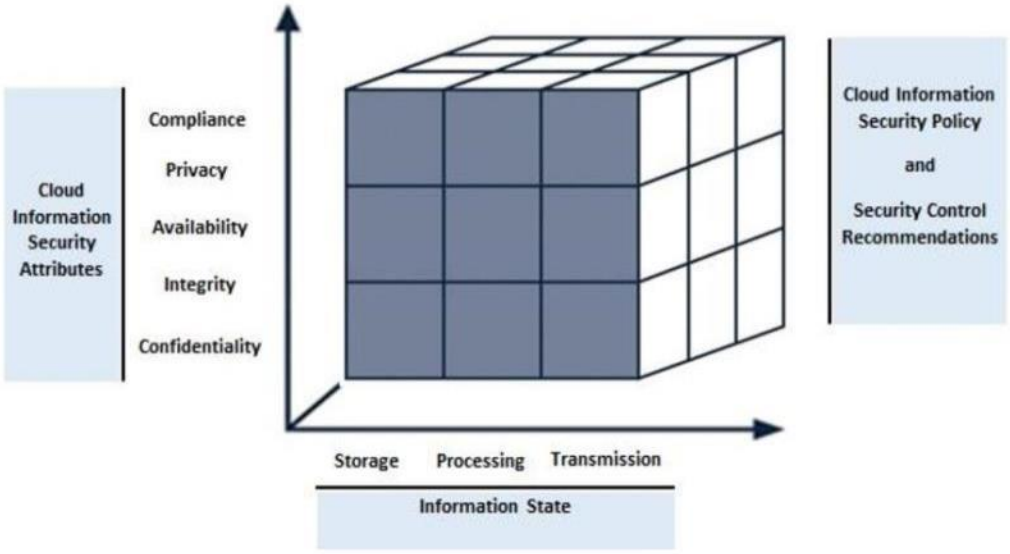


Figure 2 The information security, privacy, and compliance (ISPC) three-dimensional (cubic) model.

4.2 Readiness Factors (RF)

After determining the ISPC areas of concern, the next step is to identify and determine what factors affect information security, privacy, and compliance performance in a cloud environment. Typically, these factors are derived from the three critical assets, namely people, technology, and information. These factors can best be determined by involving individuals from different areas of the organization in choosing the readiness factors to be measured. Some important factors affecting cloud ISPC readiness are:

- **Organization Mission and Vision:** organizations tend to be reactive to information security and privacy incidents instead of being proactive. Experts agree that clear objectives are essential in adopting and implementing an effective proactive information security program [20]. McKay [21] further states that if the mission is not sufficiently defined, an organization will have difficulty securing its information and enforcing information security, privacy, and compliance policies.
- **Confidentiality:** in order to prevent unauthorized cloud information access and disclosure, an organization must implement strong authentication methods such as two-factor authentication. It can also limit user access to only the information required to complete a certain task i.e., role based access control.
- **Integrity:** an organization must implement measures to protect the integrity of its critical assets from unauthorized modification e.g., encrypting data.
- **Availability:** cloud resources are prone to attacks such as denial of service (DoS) that prevent customer access. Thus, service level agreements must address the issues of service interruption and maintenance. For critical assets, authorized parties should be able to access the data at any time.
- **Training, Awareness, and Education:** in order to deal with the ever-changing cloud services and security environment, personnel should have continuous training, awareness and education programs. Katz [22] determined that personnel are the greatest security threat with many incidents originating within the organization. Thus, ongoing education and training programs are essential to achieving information security, privacy, and compliance program targets.
- **Management Support:** typically, senior management are not information security experts. Thus security awareness must be provided so they understand the importance and criticality of information security, privacy, and compliance. This will ensure sufficient support and resources for policy enforcement.
- **Information Security, Privacy, and Compliance Policy:** this policy identifies the critical assets with a detailed explanation of what is

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

acceptable (and also unacceptable) behavior to ensure security, privacy and compliance. It is the key to effective information security management. The creation of an information security policy is a key step in determining the necessary requirements for cloud security.

Organizations tend to (unintentionally), overlook some critical areas and factors that require security, privacy, and compliance controls. This is typically due to a lack of coordination of knowledge, documentation, training and awareness, and expert assessment. In addition, policy enforcement and management support is a key element in effective asset security. Sections 4.1 and 4.2 outline activities that enable the sharing and cordination of knowledge needed to determine areas which may pose a threat to information security, privacy, and/or compliance. It is essential to identify those areas and factors that may impact cloud security in order to assess the readiness of an organization to mitigate, respond, and recover from potential risks.

Factor name: (e.g., Confidentiality of Corporate Intellectual Property (IP))					**Date:** __/__/20__
Owner: (e.g., inventors and users of IP such as research and development personnel) **Involved parties:** (e.g., intellectual property office (IPO), information security department, operations and development personnel, internal auditors, and public relations personnel)					
Version: 1.0			***Revision: 1.1***		
LEVEL #	**1**	**2**	**3**	**4**	**5**
DEFINITION	- The organization does not have info mation security documents. - The organization lacks comprehensive awareness of its information security, privacy, and compliance requirements. - The organization does not have adequate resources i.e., technology and, personnel, for effective information security.	- The organization has information security, privacy, and compliance policy documents. - The organization reacts to incidents, cyber attacks, and asset exposure risks. - The organization does not update or share policy documents. - Training and awareness programs are not provided. - Security, privacy, and compliance solutions are not effective.	- The organization has clear and communicated information security, privacy, and compliance policy documents. - Some documentation and procedures are shared and updated. - Training, awareness and education programs have been established, but are infrequent. - Security, privacy, and compliance solutions are focused on only legal requirements.	- The organization has clear, well defined, and communicated information security, privacy, and compliance policies, procedures, duties, and guidelines. - Documentation is updated and shared among appropriate personnel only for key issues. - Training, awareness and education programs have been established with a focus on mitigation and response to key issues. - Security, privacy, and compliance practices are focused on the issues facing critical assets.	- The organization has clear, well defined, and communicated information security, privacy, and compliance policies, procedures, duties, and guidelines with dynamic and agile updates. - Documentation is regularly updated, backed up, shared, and easily located. - Training, awareness and education programs are promoted by incentives and are tailored to accommodate effective learning. The focus is on a broad range of issues. - Security, privacy, and compliance solutions can proactively respond and recover from potential threats and risks.
READINESS LEVEL	**Not Prepared**	**Reactive**	**Basic Readiness**	**Moderate Readiness**	**Optimized Readiness**
CURRENT STATE			**X**		
TARGET STATE					**X**
REMARKS					

Table 1 Measurement levels for cloud ISPC readiness

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

4.3 Readiness Assessment (RA)

Once the critical readiness factors have been established, the current setting for each factor is determined. For instance, the level of training used to improve and certify employee skills in handling information security, privacy, and compliance controls. The RA outputs are:

- The current state of the security, privacy, and compliance controls and requirements.
- The desired state of the information security, privacy, and compliance program.

Once a cloud organization has the required security services in place and has achieved the desired level of security readiness, it should be continuously monitoried to ensure this level is maintained. Table 1 provides an example of the readiness levels in satisfying cloud information security, privacy, and compliance requirements for a factor. Five levels are given for the purposes of evaluating the readiness of factors such as those in Section 4.2. The table is structured as a template to indicate the current and desired states for each factor. Remarks and recommendations regarding these levels should be added to provide a clear indication of the situation and an accurate assessment of readiness.

4.4 Feasibility Analysis (FA)

To determine if cloud services for the support of ISPC systems are beneficial in terms of cost, operation, effectiveness, and security, a feasibility analysis (FA) is incorporated in the ISPC readiness model. The FA is executed once the current and potential (i.e., after cloud migration) ISPC services have been assessed.

The FA consists of two parts:

- *Technical Feasibility*:
  This part contains the technical requirements to meet the desired ISPC readiness. The organization should:
  - Ensure the compatibility of current ISPC components for migration to cloud services.
  - Ensure the chosen cloud technology has the capacity to handle the desired ISPC targets, and can solve any current/outstanding ISPC issues.
  - Document the resources required e.g., time, manpower, and facilities, to transfer current ISPC systems to the cloud, and determine if they are available.
  - Document the issues facing the migration plan. For example, some legacy systems and/or source code may not be supported by the cloud service model. In this case, alternative solutions should be investigated and implemented prior to migration.

- *Business Feasibility*:
  This part considers the economic factors and policies associated with migration. The organization should:
  - Ensure that the cost of ISPC migration is justified and the migration conforms to the information security, privacy, and compliance policy.
  - Revise the ISPC policy document to reflect changes such as the inclusion of the cloud secure SLA agreement in support of ISPC operational performance and availability.

The FA is usually conducted using focus groups and experts to provide an informed decision on whether to migrate to the cloud and the associated modifications required to current ISPC systems. The technical FA is conducted by system analysts and the business FA is conducted by auditors and experts in the areas of organizational, financial and market issues. The FA can use questionnaires and interviews as necessary to engage personnel in sharing objectives and concerns. This will ensure well informed decisions are made.

4.5 Readiness of the Migration Plan (RMP)

The RA and FA assessments are key factors in the decision to migrate to the cloud. The migration plan should encompass the vision of the organization to avoid any deviations from the mission objectives. Before migration, all issues i.e., compatibility, integration, and lock-in, must be resolved to ensure a successful transition of the information systems to a cloud provider or a new cloud provider. Further, the migration plan should not be implemented until all ISPC requirements have been addressed in accordance with the readiness model. The final migration readiness document should be signed off by all key participants to ensure accountability and continued support for security operations, improvements, and unforeseen risks.

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

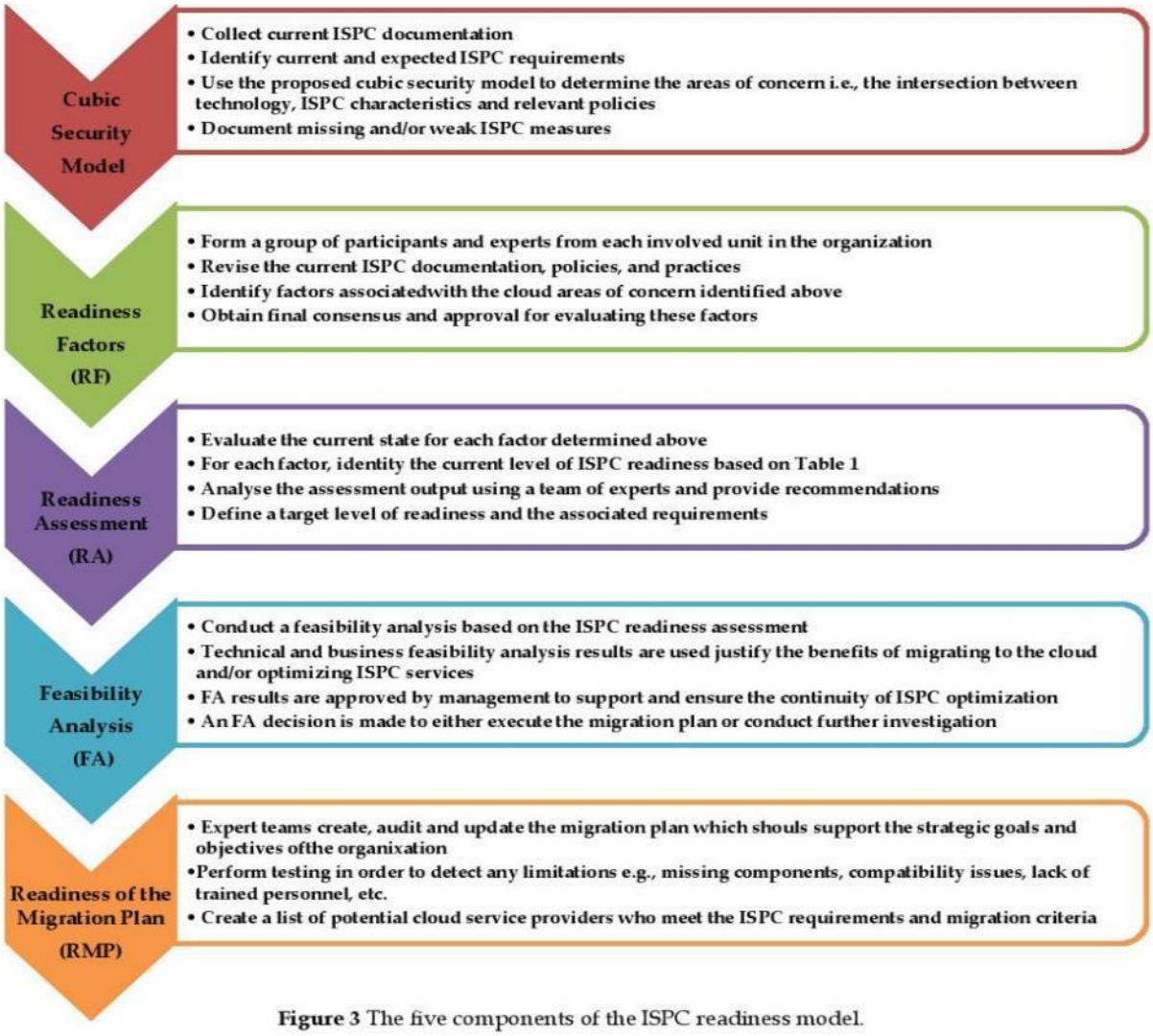


Figure 3 The five components of the ISPC readiness model.

4.6 ISPC Readiness Flowchart

Figure 4 presents a flowchart detailing the implementation of the ISPC assessment in accordance with the proposed cubic model, risk assessment methodology, and readiness levels. This assessment indicates management support, awareness, and commitment to improving ISPC practices and policies. Experts from all departments involved in the assessment are expected to participate in revising current ISPC policies and practices. This group is responsible for determining the technical and organizational factors impacting ISPC performance based on the risk assessment (RA) results. The information obtained from the previous steps will assist them in determining the current and desired ISPC readiness states. Finally, a feasibility analysis (FA) is conducted to ensure that the time and cost in implementing the migration plan is justified. ISPC policies and practices are updated as required. Ongoing monitoring of the ISPC systems is recommended to ensure that compliance and security performance expectations are maintained.

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

5 Discussion

In this section, the advantages of the proposed ISPC readiness model are discussed. It is also shown that the organization requirements identified in Section 2 are satisfied.

The main objective of the proposed ISPC readiness model is to provide methods and techniques to support organizations in evaluating their current ISPC readiness against cloud specific threats. It can be used by organizations that have or are considering IT migration to the cloud. This readiness model provides a sustainable assessment methodology to support informed decision making with regards to cloud migration and ISPC system optimization. Tools are provided to measure the current and desired ISPC readiness of an organization in facing potential known or new threats during and after transitioning to the cloud.

The ISPC readiness model enables an organization to evaluate readiness internally or with external experts such as a trusted third party. If the ISPC expertise is sufficient, it is recommended that the readiness be evaluated internally to ensure maximum privacy and confidentiality of the assessment results. Otherwise, a trusted third party should be employed to conduct the ISPC assessment using the proposed readiness model. Further, measures such as confidentiality and non-disclosure agreements (CNDAs) should be used to protect intellectual property (IP) from risks such as disclosure e.g., sharing ISPC assessment results and migration plans with other organizations such as competitors can have very deliterious effects.

Table 1 for readiness assessment was developed in accordance with the SSE-CMM maturity levels for enhancing information security systems. However, the SSE-CMM does not prescribe a process for ensuring successful implementation of a proactive ISPC system in the cloud or elsewhere. Thus, this table provides a template that can be used to assess each factor affecting ISPC readiness to determine current and desired readiness levels. Expert teams should be formed to ensure accurate readiness evaluation.

It is clear that ISPC readiness cannot be determined based on a single factor or single technique. A multifaceted holistic approach incorporating multiple factors and techniques is required to ensure the success of migration to the cloud. The flowchart in Figure 4 illustrates the detailed sequence of steps in applying the readiness model. This shows that ISPC readiness model is an iterative, collaborateve process which allows for continuous evaluation and updates. The results are shared among all involved departments to enable not only effective ISPC optimization but also a well-informed and self-aware organizational culture.

6 Conclusion

Many organizations are either considering or making the move to cloud services due to the ever-increasing benefits. As a consequence, IT security and privacy, and compliance with regulatory requirements, have become an important research area to address the concerns and limitations of cloud computing environments [3].

This paper proposes an information security, privacy, and compliance (ISPC) readiness model that contributes to the goal of improved cloud security. This readiness model is multifaceted. It includes a cubic ISPC model for identifying the areas of concern with regards to to information security, privacy, and compliance requirements. This model was designed to audit existing ISPC documentation and determine the key factors affecting current ISPC settings. The assessment of the current ISPC implementation is in accordance with our proposed risk management framework for cloud services [10] and based on the ratings presented in Table 1. The ISPC readiness model captures the organization cognitive attitudes towards building, operating, and managing secure, compliant, and trusted cloud computing services. Specifically, it captures how personnel react to security threats and incidents in an effort to determine their ability to effectively operate ISPC systems. In this regard, knowing the levels of security training, awareness and education is critical.

The proposed ISPC readiness model is not limited to organizations considering migrate to the cloud, but can also be employed by those seeking to develop or improve ISPC programs. In addition, the model can be used to assess ISPC assets and factors contributing to readiness such as culture cognition and awareness. For instance, the reaction of personnel to information security, privacy, and compliance threats can be evaluated. Expert groups are used to determine the factors affecting ISPC systems and the desired levels of ISPC readiness. These groups provide recommendations for achieving these desired levels based on the current readiness assessment results and more importantly on the support from the organization to continue improving their ISPC program.

The ISPC readiness model allows an organization to check for any cloud services compatibility issues with current ISPC systems in order to ensure successful implementation of a migration plan. For organizations currently employing cloud services, this model can be used to optimize ISPC systems and establish a risk-aware culture which promotes proactive activities.

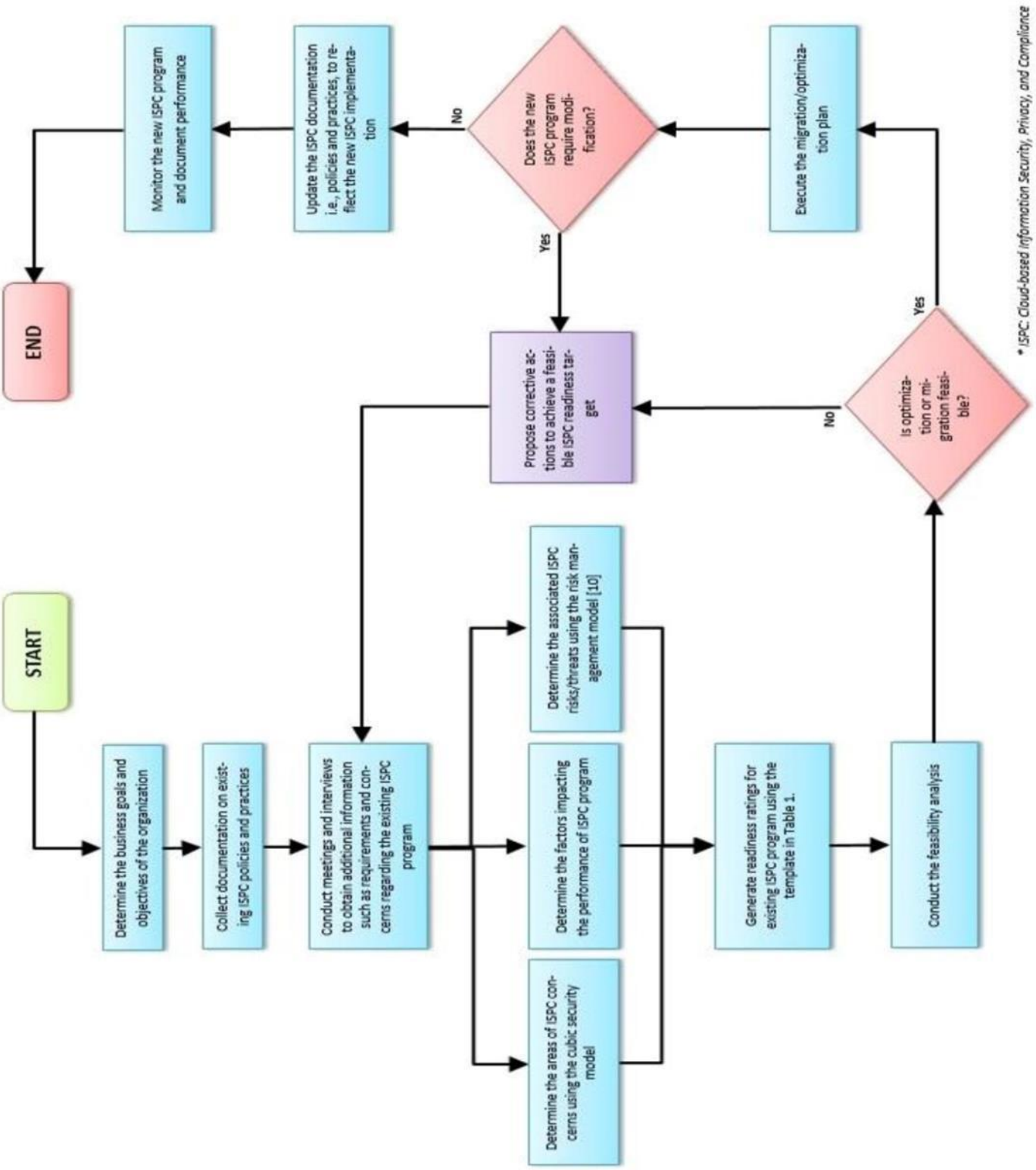


Figure 4 The ISPC readiness model.

INTERNATIONAL JOURNAL OF FUTURE GENERATION DISTRIBUTED SYSTEMS (IJFGDS)
Vol.4, No.4, December 2014, ISSN 2289-3369
WWW.IARTC.NET

REFERENCES

[1] S. Murugesan, "Cloud Computing Gives Emerging Markets a Lift," *IEEE Computer Society on IT Professional,* Vol. 13, No. 6, pp. 60-62, December 2011.

[2] R. Chandramouli, and P. Mell, "State of Security Readiness," *ACM Crossroads*, Vol. 16, No. 3, pp. 23-25, March 2010.

[3] G. Sibiya, T. Fogwill, H. S. Venter, and S. Ngobeni, "Digital Forensic Readiness in a Cloud Environment," *IEEE Conference on AFRICON*, pp. 1-5, September 2013.

[4] J. Morin, J. Aubert, and B. Gateau, "Towards Cloud Computing SLA Risk Management: Issues and Challenges," IEEE Hawaii International Conference on System Science, pp. 5509-5514, January 2012.

[5] F. F. Alruwaili, and T. A. Gulliver, "SOCaaS: Security Operations Center as a Service for Cloud Computing Environments," *International Journal of Cloud Computing and Services Science*, Vol. 3, No. 2, April 2014.

[6] Asia Cloud Computing Association, "Cloud Readiness Index," *Asia Cloud Computing Association 3rd CRI Report*, http://www.asiacloudcomputing.org/research/cri2014, 2014, Last viewed (15-09-2014).

[7] World Economic Forum, "Advancing Cloud Computing: What to Do Now? Priorities for Industry and Governments," *World Economic Forum*, http://www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf, 2011, Last viewed (30-10-2014).

[8] C. Loebbecke, B. Thomas, and T. Ullrich, "Assessing Cloud Readiness: Introducing the Magic Matrices Method Used by Continental AG," *Springer on Governance and Sustainability in Information Systems: Managing the Transfer and Diffusion of IT*, Vol. 366, No. 2, pp. 270-281, September 2011.

[9] G. Conway, and E. Curry, "Managing Cloud Computing: A Life Cycle Approach," *CLOSER International Conference on Cloud Computing and Services Science*, pp. 198-207, April 2012.

[10] F. F. Alruwaili, and T. A. Gulliver, "Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services," *International Journal of Future Generations Distrubuted Systems*, Vol.1, No. 2, Septemeber 2014.

[11] F. F. Alruwaili, and T. A. Gulliver, "SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services," *International Journal of Cloud Computing and Services Science*, Vol. 3, No. 4, August 2014.

[12] ISO, and IEC, "Information Technology Systems Security Engineering—Capability Maturity Model (SSE-CMM, ISO/IEC 28127)," International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC), 2002.

[13] R. Kurdi, A. Taleb-Bendiab, M. Randles, and M. Taylor, "E-Government Information Systems and Cloud Computing (Readiness and Analysis)," IEEE International Conference on Developments in E-systems Engineering, pp. 404-409, December 2011.

[14] D. C. Wyld, "Moving to the Cloud: An Introduction to Cloud Computing in Government," *IBM Center for the Business of Government*, November 2009.

[15] A. K. Hosseini, D. Greenwood, J. W. Smith, and I. Sommerville, "The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise," Journal of Software: Practice and Experience, Vol. 42, No. 4, pp. 447-465, April 2012.

[16] B. Bailey, "Cloud Computing may Create New Venues for High-Tech Criminals," *San Jose Mercury News,* http://www.mercurynews.com/businessbreakingnews/ci_12812412?nclick_check=1, Septemeber 2009, Last viewed (31-10-2014).

[17] E. Estevez, T. Janowski, I. Marcovecchio, and A. Ojo, "Establishing Government Chief Information Officer Systems: Readiness Assessment," *ACM Proceedings of the International Digital Government Research Conference: Digital Government Innovation in Challenging Times,* pp. 292-301, June 2011.

[18] S. Dutta, and I. Mia, "ICT for Sustainability," *World Economic Forum on Global Information Technology Report 2009–2010 World Economic Forum,* 2010.

[19] T. Obi, "Waseda University World e-Government Ranking," *Research report of the Waseda University Institute of e-Government*, http://www.waseda.jp/eng/news10/index.html, January 2010, Last viewed (31-10-2014).

[20] M. Al-Awadi, and K. Renaud, "Success Factors in Information Security Implementation in Organizations," *International e-Society Conference International Association for Development of the Information Society*, pp. 169-176, July 2007.

[21] J. McKay, "Pitching the Policy: Implementing IT Security Policy through Awareness," *USA: SANS Institute*, http://www.giac.org/paper/gsec/3223/pitching-policy-implementing-security-policy-awareness/105199, July 2003, Last viewed (29-10-2014).

[22] F. H. Katz, "The Effect of a University Information Security Survey on Instruction Methods in Information Security," *ACM Proceedings of the Annual Conference on Information Security Curriculum Development,* pp. 43-48, September 2005.

AUTHOR BIOGRAPHIES

Fahad F. Alruwaili is a faculty member in the Computer Science Department of the University of Shaqra, Saudi Arabia. He is an information security and computer networks consultant with over twelve years of research and development experience. He earned his BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he received the MS degree in Computer, Information, and Network Security with first class honours from DePaul University, Chicago USA. In 2011, he received the MS degree in Information Systems and Technology from Claremont Graduate University, Los Angeles USA with first class honours. He is currently working towards the PhD degree in the Department of Electrical and Computer Engineering at the University of Victoria, BC, Canada. His research interests are in the technical and theoretical aspects of information security and data privacy.

T. Aaron Gulliver received the PhD degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.

Chapter 8

SecSDLC: A Practical Life Cycle Approach for Cloud based Information Security

As published in *International Journal of Research in Computer and Communication Technology*,
February 2015

This article appeared in Vol. 4, Issue. 2, published by *International Journal of Research in Computer and Communication Technology*, *Copyrighted to © IJRCCT.ORG Publisher, India*.
The attached copy is furnished to the author for internal non-commercial research and education use, including for instructions of the authors institution and sharing with colleagues.
Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.
In most cases authors are permitted to post their version of the article to their personal websites or institutional repository. http://ijrcct.org/index.php/ojs

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

IJRCCT International Journal of Research in Computer and Communication Technology ISSN (O) 2278-5841 ISSN (P) 2320-5156

SecSDLC: A Practical Life Cycle Approach for Cloud-based Information Security

Fahad F. Alruwaili and T. Aaron Gulliver

Department of Electrical and Computer Engineering
University of Victoria,
P.O. Box 1700 STN CSC
Victoria, BC V8W 2Y2 Canada
{fruwaili,agullive}@ uvic.ca

Abstract—**Cloud computing services offer significant benefits to information technology (IT) systems such as reduced cost and shorter implementation time compared to traditional IT environments. However, the cloud multi-tenancy and web-enabled architecture creates a complex environment in which to develop and manage information security and compliance programs. At the enterprise level, risk and threat management can be an issue if it fails to protect cloud confidentiality, integrity, and availability (CIA). In this paper, a practical cloud security system development life cycle (SecSDLC) methodology is proposed to provide a holistic approach to effective and efficient cloud information security. The SecSDLC is based on industry best practices, and widely used and accepted methodologies such as waterfall SDLC, and NIST SP 800-64 revision 2 information security. Our previously developed solutions for cloud intrusion detection and prevention, security system monitoring, secure SLA, and compliance auditing are incorporated into the SecSDLC. A formal methodology is proposed to address concerns regarding cloud security and compliance requirements. The goal is to increase the probability of a successful information security program and reduce the likelihood of missing or inadequate components that may compromise cloud information security.**

Keywords—**System Development Life Cycle (SDLC), Security Operations Center (SOC), Information Security Design and Development, Cloud Provisioning, Risk Management, Cloud Security Services, Service Level Agreement (SLA).**

I. INTRODUCTION

Cloud computing services are considered to be the next generation technology based on a distributed computing platform that enables on-demand and dynamic provisioning of information technology (IT) resources. These services are offered as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), and leverage virtualization and internet technologies. Cloud IT capabilities are delivered to customers using a pay as you use model i.e., cloud customers can purchase resources as required, enabling agile adaptation to new IT demands. Cloud resource delivery eliminates the burden of establishing an IT system with the associated infrastructure and personnel [1], [2].

In 2010, the Information Systems Audit and Control Association (ISACA), an international group of professionals focused on IT governance, conducted a risk and reward survey [3] via an online poll of 1,809 members. The results obtained confirm that many organizations are considering migrating to cloud computing services to reduce IT costs. However, the benefits are often outweighed by the security threats and compliance requirements facing cloud customers and service providers [4].

When cloud computing service models were first developed, the focus was primarily on service performance, convenience, on-demand and rapid deployment, and functionality. Conversely, issues such as information security and cloud risk controls were given a low priority [5]. Consequently, there are concerns regarding cloud service reliability, security, availability, privacy, performance, and the security measures contained in service level agreements (SLAs) [6], [7], [8], [9], it was shown that there are significant costs associated with cyber-attacks due to lost productivity, revenue and customer trust. Cloud service interruption is considered one of the greatest risks facing cloud service providers and customers. In February 2008, Amazon cloud services were down for six hours and their storage service (S3) and elastic compute cloud (EC2) services were unavailable for three hours [10]. In early 2009, Google webmail services (Gmail) was out of service for three hours preventing more than 113 million subscribers from accessing their email and document (Google Docs) services [10]. In addition,

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015
ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

Microsoft cloud services (i.e., Hotmail, SkyDrive, and Office 365) were unavailable for three hours in September 2011 [11].

It is clear that a well-defined cloud information security program is needed to encourage the adoption of cloud services. Further, it is important that organizations considering migrating to the cloud have thorough knowledge of the information security programs of potential service providers. This ensures an understanding of the information security safeguards that have been deployed and their effectiveness against cloud threats. It is also crucial that both service providers and customers understand the life cycle of cloud security services. This includes initiating, analysing, designing, implementing, and maintaining security programs, and provides an effective means of developing and evaluating cloud information security systems [12]. There are serious concerns regarding the risks and threats that can affect cloud information security and data privacy. Further, the cloud multi-tenancy architecture and multi-layer service model have spawned new and complex threats that could be catastrophic to cloud customers. For example, an exploited vulnerability in the IaaS cloud model could lead to service disruption and system unavailability [13]. Thus there are significant challenges in developing, provisioning, and managing secure cloud resources [14].

Cloud customers are attracted by the low cost, flexible, accessible (access from anywhere at anytime), and agile (quickly add or remove IT resources) cloud services. However, these benefits are at the expense of limited or unknown protective measures [11]. In addition, there is great concern regarding information security, data ownership, lack of interoperability, and lock-in due to the lack of cloud security controls and standardization [14]. There are a myriad of cloud service providers employing various approaches to security. Thus, potential customers have trust issues regarding the quality and effectiveness of the information security programs of service providers. Cloud customers without sufficient knowledge of these programs may suffer severe consequences as a result of a security incident. Therefore, organizations should review the information security policies and programs of current or potential cloud service providers. This review should include a comprehensive assessment of the programs implemented to ensure adequate security is provided for their critical information systems and services [15].

Protection from security issues facing cloud customers and service providers such as cyber threats, security compliance and regulatory requirements, and data availability and confidentiality, depends almost entirely on the information security programs of the cloud service providers. In this paper, a security system development life cycle (SecSDLC) approach is presented to plan, design and implement information security within the domain of a cloud service provider. The goal is to address and counter the security risks and threats associated with cloud computing services. It is based on relevant security controls and widely accepted security practices developed by the Cloud Security Alliance (CSA) and our prior work on a security operations center for cloud computing [16], [17]. The CSA threat security control recommendations are aligned with industry security standards and guidelines such as NIST SP800-53, COBIT, ENISA IAF, HIPAA, ISO 27001/27002, NERC CIP, PCI DSS, and FedRAMP [18], [19].

The detailed SecSDLC phases provide an effective approach to the design and implementation of a proactive cloud information security system. These six phases are presented in Table 1. They include security control guidelines and recommendations to address cloud security concerns. This table applies to security program development by both cloud customers and service providers. The SecSDLC is based on the widely used and accepted system development life cycle methodology. The goal is to aid cloud organizations in making informed decisions regarding the development and implementation of information security systems. This is achieved via collaboration between expert teams, IT personnel, and business units to rigorously review and approve the security system development throughout its life cycle. This allows for the identification of security deficiencies so that corrections can be made.

II. Related Work

Implementing effective information security systems across different cloud layers is a significant challenge. The National Institute of Standards and Technology (NIST) has released publication SP 800-64 revision 2 which provides recommendations for organizations planning to develop and implement information security programs [18]. In addition, version 3.0 of the CSA cloud controls matrix (CCM) contains a number of baseline controls for cloud computing services. These controls are mapped to industry standards, regulations and frameworks, such as NIST, PCI DSS, HIPAA and COBIT [19]. The CSA also provides a governance, risk management, and compliance (GRC) stack to assess both private and public cloud services against industry established best practices, standards and compliance requirements [19].

Breiter and Behrendt [20] described the life cycle of cloud services with regards to managing information technology infrastructure processes. They proposed simplifying cloud service provisioning through ensembles i.e., a centralized and managed cloud resources pool. This enables straightforward and scalable provisioning with lower administration and management costs compared to provisioning from heterogeneous and dispersed cloud resources.

Kao et al. [21] presented a self-governance framework for both government and industry based on the cloud

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015
ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

system development life cycle. Their framework considers the threats and risks to the cloud that must be monitored and audited for compliance with legal and regulatory requirements. However, they do not provide a holistic approach to the security system development life cycle, in particular no steps or models are proposed for implementing a cloud specific information security system.

The authors in [22] emphasised the importance of cloud resource provisioning and the associated issues concerning security, privacy, reliability, access and regulation. They explored policy (e.g., information security policy) issues with regards to cloud service provisioning and the lack of guidance which is an impediment to the adoption of cloud services. Two approaches were presented to establish cloud computing standards, regulation by a designated government agency or greater detail in service level agreements (SLAs), in an effort to resolve cloud policy issues. These enable the development of policies, regulations, and even laws to address these issues. The focus is on the lack of policies and the limitations in existing laws and regulations, while the development and implementation of a life cycle for cloud security programs was not considered.

Ferrer et al. [23] proposed a life cycle for cloud services which includes their design, development, and operation. Only the optimization of service provisioning within the IT infrastructure of a cloud service provider was considered. Further, five high level challenges that must be addressed for wider adoption of cloud services were discussed. However, the design and implementation of a life cycle for cloud security was not considered.

The CSA also proposed a data security life cycle [24]. It is composed of six processes denoted produce, store, use, share, archive and destruct. However, it only provides security management guidelines for the data life cycle in cloud computing. While this is an important element of an information security program, no methodology was proposed for the information security life cycle.

III. The Cloud Security System Development Life Cycle

The security system development life cycle (SecSDLC) is a key component of an effective cloud information security program. It addresses all development phases i.e., planning and investigation, analysis and design, user and system requirements, implementation, monitoring and support. This ensures that the security objectives and tasks are met and followed. The SecSDLC does not terminate until the security program and its associated applications are retired. It is an iterative process so that changes in the cloud components (e.g., policies, resources, and business goals), can be incorporated into the life cycle as required. Unlike traditional approaches, the SecSDLC enables a return to the previous phase if a change is required [34]. Significant changes may require that the process be restarted.

Recently, there has been significant effort by governments to guard data privacy and prevent security breaches to cloud services [13]. The SecSDLC is tailored to support the implementation of effective information security in cloud computing environments.

SecSDLC Methodology

The SecSDLC methodology is proposed to ensure proper design and implementation of information security by a cloud organization. It provides a formal approach to solving security problems based on a structured sequence of phases. This ensures a systematic process and avoids missing items (e.g., risks, threats, technical components, controls, policies, business unit integration, and cloud assets), that may lead to compromised security.

To increase the probability of a successful cloud information security program, the phases of the proposed methodology must be established, documented, and agreed upon by a team of individuals (i.e., cloud asset owners, administrators, risk control units, information security personnel, and stakeholders). The SecSDLC has six phases which are discussed below and presented in Table 1.

A. ***PHASE I:*** *Cloud Security Program Initiation and Investigation*

The SecSDLC is initiated with the intent to reduce costs and operational overhead by migrating to cloud services, or in response to a specific information security requirement (e.g., incident, risk control, change request, or compliance request). The investigation phase begins once a cloud customer or service provider has defined clear roles and reasons for the security program. Some examples of roles and reasons are:

- *To appropriately protect data integrity, availability and confidentiality.*
- *To minimize exposure to legal and compliance risks.*
- *To demonstrate compliance with internal policies, laws, and regulatory requirements.*
- *To demonstrate management support for the program.*
- *To reduce the costs associated with acquiring information security resources.*

The process begins with management dictating the scope, outcomes, and goals of the program in accordance with the information security policies of the organization. A set of criteria are established to specify the program objectives and constraints (limitations). During this phase,

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

the confidentiality, integrity, and availability (CIA) for cloud users and system requirements are developed according to information security policies and directives.

The last task in this phase is to conduct a preliminary cost benefit analysis to justify the procurement of cloud security services. This analysis is performed to ensure that the cloud information security program is worth the effort, time, and investment. It will also determine if the organization has the necessary resources and commitment to undertake the program.

B. ***PHASE II:*** *Cloud Security Program Requirements and Risk Analysis*

During this phase the preliminary user and system security requirements developed during the previous phase are analysed and revised if necessary. These requirements are checked against current security controls and risk factors taking into account the scope and objectives of the program. This phase has two steps:

- ***Cloud User and System Requirements Analysis***

  The results of the initiation and investigation phase are passed to the development team to conduct an analysis of the current cloud information security programs and their architecture. In particular, the programs are checked for current threats and control mechanisms. Any legal (e.g., privacy laws) and organizational requirements and issues (e.g., disconnect between business units) that could affect the design and implementation of the program are also identified.

- ***Cloud Risk Analysis***

  Risk analysis is the process of developing an asset inventory and identifying, assessing, and evaluating the associated risks, threats, and vulnerabilities. This ensures that current and perceived threats are addressed by an adequate risk control strategy to eliminate or limit their impact on cloud assets and resources.

  A detailed understanding of the information security policies and current security controls is vital. Analysing the technical, organizational, and legal risks facing cloud services and organizations is considered the most important task in the SecSDLC. The results of this analysis are used to refine security control policies and ensure all critical cloud assets are identified, classified, monitored and protected. The feasibility analysis conducted in Phase I is updated according to the results of this phase. Thus, at the end of Phase II existing cloud security policies and programs have been thoroughly evaluated and revised. In addition, all current risks (i.e., organizational, technical, and legal), have been identified.

C. ***PHASE III:*** *Development, Provisioning, and Procurement of Cloud Security Services*

In this phase, the user and system requirements and specifications are used to design the cloud security program. If the organization approves the design, development, and implementation of the information security program, then it is deployed, operated, and maintained using one of the provisioned cloud offerings i.e., PaaS or IaaS. Another option is to procure a complete cloud security solution that meets the specifications as outlined in a request for proposal (RFP) document.

- ***Logical Design***

  The logical design produces a map for the information security program implementation based on the Phase II analysis. The design team develops and revises the security plans (i.e., incident response, disaster recovery, and business continuity plans). Moreover, it generates a list of cloud security solutions that meet the program analysis and risk assessment requirements from Phases I and II. These are used in the physical design to determine the best cloud security solution.

- ***Physical Design***

  In the physical design, the most appropriate cloud services that support the Phase II requirements and the logical design are selected. This is the most suitable cloud vendor or service provider, platform, application and data support that meets the security program user and system requirements. The logical design is used in the physical design, so it should be revisited to ensure any changes from the physical design are incorporated. The key personnel (i.e., asset owners, administrators, risk control unit, information security personnel, and stakeholders) should review and approve the final design prior to implementation. In some cases, a thorough test of the selected cloud solution is required prior to implementation in order to verify that the security requirements are satisfied. This is called proof of concept (POC) or user acceptance testing (UAT). It can also be used to verify the security functionality and correct any problems encountered (e.g., software and functionality issues, or missing components).

At the end of this phase, the feasibility analysis should reflect the readiness of the organization to implement the selected cloud security solution. Thus management is in a position to determine whether or not the cloud security program should be implemented.

D. ***PHASE IV:*** *Program Implementation*

During this phase, the cloud security solution is implemented according to the results of the previous

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

phases. The solution can be locally developed and then outsourced to run on top of an IaaS or PaaS cloud service model. Alternatively, an existing cloud solution can be acquired. During and after implementation, the security solution should be continuously monitored and tested to ensure proper rollout.

If any changes are made during implementation, the documentation (and feasibility analysis if necessary), should be updated. Cloud security personnel (i.e., system and network administrators, operators, security analysts, and risk auditors) must receive suitable training and education to appropriately implement, operate, support, and monitor the security program. This will reduce the number of risks and threats due to personnel errors.

E. ***PHASE V:*** *Program Operation and Maintenance*

The operation and maintenance phase is very important due to its criticality to the success of the security program. After implementation, ongoing support, administration, monitoring, modification, updating, and repair are required. This should be done proactively so that incidents can be identified quickly and appropriate responses proposed. As new cloud service models emerge (e.g., SaaS, PaaS, IaaS, security operations center as a service (SOCaaS), and communication as a service (CaaS)), new cloud threats will evolve, so the security program should have sufficient agility to adapt to new threats. Continuous and vigilant monitoring and maintenance of the security program ensures efficient and reliable security system operation. Further, ongoing refinements and baselining with new and innovative cloud security technologies are advised.

During this phase and as a part of the maintenance program, upgrades and patches will be required. To avoid any compatibility and/or service disruption issues, it is suggested that these changes be tested in a non-production environment prior to implementation.

The two critical functions in this phase are as follows:

- ***Configuration and Change Control***

  Periodic monitoring and testing is required to ensure compliance with organizational, technical, and legal needs. In addition, change management (CM), change control and/or configuration change (CC) requests and status should be documented. CM is responsible for processing cloud service changes to promote new business initiatives without affecting current cloud services. CC on the other hand is the process i.e., change request, submission, analysis, decision making, approval, and update, of implementing the changes. The CM and CC are coupled to ensure proper handling and maintenance of changes to the cloud security requirements.

- ***Third Party Components and Extensions***

  Some cloud service providers outsource their cloud infrastructure to third party cloud providers. If the selected security solution involves third party cloud resources, then the cloud customer should be informed and able to verify security integration and cross-system service functionality. Usually, this is accomplished through integration modules between the two service providers (e.g., load balancers, network security monitoring agents, and IP address and authorization management).

F. ***PHASE VI:*** *Retirement and Deprovisioning of Cloud Security Services*

Cloud services provide on demand provisioning of IT resources that support information security programs. Deprovisioning is a key component of the cloud security program life cycle. This phase ensures that cloud resources (e.g., cloud accounts) are properly and systematically deactivated or deleted. For example, if personnel involved in operating the information security system leave the organization, their accounts must be disabled/deleted and entitlements revoked to avoid risks associated with insider threats (e.g., to prevent possible attacks by disgruntled former personnel). As another example, if a cloud firewall device is scheduled to be decommissioned from the security system, physical removal of the device is not sufficient. The organization should apply an appropriate removal procedure to the firewall reusable configurations (i.e., names, accounts, access lists, and security assignment roles) and trusted channels from all interconnected systems. To remove a database and virtual server from the cloud infrastructure, the following tasks must be performed:

- *Perform a full backup.*
- *Stop database services.*
- *Update the domain name service (DNS) to remove the database and virtual server names and IP addresses.*
- *Perform network deprovisioning.*
- *Disable database port listeners.*
- *Remove related data files, control files, scripts and utilities.*

The decommissioning and disposal policies and procedures must be specified clearly and communicated to the cloud customer and service provider. Prior to retiring or replacing a security program, the following procedures must be carefully revised and updated:

- *Cloud software and hardware removal/disposal.*
- *Cloud media sanitation.*
- *Cloud data/information retention.*
- *Cloud data and application transfer.*

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

Each of these procedures should provide detailed instructions for the appropriate removal, transfer, and deprovisioning of cloud security services according to the organization policy documents.

In this phase, there may be issues with cloud interoperability and standardization between service providers. For example, if a cloud customer wants to terminate its security program with provider A and migrate to provider B, then there may be importing and exporting difficulties due to implementation and compatibility limitations. Cloud providers are encouraged to resolve lock-in problems, i.e. customers tied to a particular cloud vendor, at an early stage to ensure customers are free from proprietary solutions and enable interoperability of cloud data and its applications.

To avoid cloud risks, customers and service providers are advised to:

- *Ensure security control procedures and guidelines are followed (typically by enforcement procedures across all SecSDLC phases).*
- *Communicate information security policies to ensure proper security awareness, skills, and behavior by personnel. This is typically done as part of a training and education program before, during and after the implementation phase.*
- *Implement adequate and continuous information security monitoring and support to eliminate or reduce cloud threats.*

Figure 1 shows the SecSDLC methodology which is a cyclic and iterative process for implementing a cloud information security program. This methodology begins with the planning and investigation phase which includes an asset inventory and documentation of all current information security policies and programs. The design discussed in Phase III provides an organized plan for implementing a security program. In Phase IV, this plan is implemented according to the design requirements. After implementation, Phase V ensures proper program operation and maintenance. The program activities are monitored in accordance with the associated policy and compliance requirements. When the program is retired or transferred to another cloud provider, the termination/disposition phase is executed to ensure all confidentiality, integrity, and availability requirements are followed to the end of the security program.

SecSDLC PHASE		SecSDLC TASKS	INFORMATION SECURITY MEASURES
1	***Initiation and Investigation***	Cloud management and the associated business units are responsible for: - Defining the program objectives, time duration, budget, and scope. - Linking the program objectives to the mission, goals, and business requirements of the organization. - Conducting a cost analysis to justify the program and its feasibility. - Evaluating existing cloud resources.	- Develop and/or revise information security policies. - Perform a preliminary risk assessment. - Inventory, categorize, and classify the cloud assets of the organization (e.g., hardware, software, data, external interfaces, and personnel).
2	***Requirements Analysis***	Cloud IT operations, information security, and risk management personnel are responsible for: - Revising the results of the initiation and investigation phase. - Performing a risk assessment (asset inventory, analysing threats, and recommend controls) using the asset identification andclassification from Phase I.	- Examine current security controls and programs. - Analyse current cloud threats and prepare for perceived ones. - Review applicable laws and regulations such as PCI DSS [26], SOX [27], FISMA [28], HIPPA [29], and SAS 70 Audit [30]. - Perform a risk assessment and analysis. For example, the risk management system developed in [31] can be used to provide a comprehensive risk assessment and control recommendations for cloud services. - Identify the relevant security program design principles. - Conduct a cost analysis to justify the program and determine its

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

		- Identifying the system and user security requirements using the results of the risk assessment. The applicable laws and regulations for compliance should also be identified. - Conducting a cost and feasibility analysis to justify the security program. - Developing a request for proposal (RFP) document (if necessary), for distribution to potential cloud providers and contractors.	feasibility.
3	***Development, Provisioning, and Procurement***	Cloud IT operations personnel are responsible for: - The user and system confidentiality, integrity, and availability (CIA) requirements. - The security assurance requirements to ensure adequate confidence that the information security program will produce the expected level of cloud protection. This can be achieved via a testing and evaluation plan. - The security solution technology selection (e.g., hardware, software, application). - Generating alternative security solutions. - Researching the market for the best service provider/vendor. - Determining whether to develop the security program or acquire it based on expert team evaluation results. - Selecting the best solution or cloud contractor. - Updating the cost and feasibility analysis.	- Ensure the security design meets the requirements defined in Phases I and II. - Apply secure design principles such as: ▪ Security in depth. ▪ Intrusion detection and prevention [32]. ▪ Risk management [31]. ▪ Security operations center [17] for larger organizations. ▪ Separation of duties i.e., having more than one person required to complete a critical task. ▪ Least privilege i.e., cloud users should not be granted more privileges than required. ▪ Secure default configurations e.g., all firewall default configurations and setup settings must be disabled. ▪ Frequently monitor and audit trusted services i.e., third party interface/integrating components. ▪ Continuity of business and recovery plans. ▪ Secure the weakest links i.e., cyber attacks often exploit the weakest points of the system e.g., privileged access via exploiting former personnel accounts is a back-door threat. Thus, accounts should be continuously audited and old accounts disabled/removed. ▪ Data privacy i.e., a comprehensive privacy program to protect personal data privacy such as the Safe Harbor framework [33]. This framework implies the following principles: - *Notice and Choice:* notice statements for the purpose of collecting data and its use. The cloud service provider should provide choices to customers with respect to data collection, storage, use, transfer, and processing in order to limit the misuse and/or disclosure of their data. - *Onward transfer:* if third party integration components and/or the sharing of data is permitted or required, all parties must subscribe to Safe Harbor principles or contractually agree to implement the same level of security according to the security policies. - *Data Access:* the data owner should have full but secure access to correct, amend, or delete information. High availability (HA) measures should be employed

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

			to provide access to information in case of system failure, cyber-attack, repair, and natural or man-made disasters. - *Data Confidentiality:* confidentiality measures should be implemented to prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure appropriate use of data. Security measures for confidentiality include data encryption while in storage or transmission, regular secure backups, access control monitoring, and intrusion detection/prevention. - *Data Integrity:* integrity measures should be implemented to ensure information is accurate, complete, and current i.e., implementing integrity checks by using hash functions, limiting hardware and software errors, and preventing system intrusions. - *Enforcement:* regularly verify that the security program complies with privacy principles. The enforcement controls should include procedures for resolving complaints with regards to privacy issues. - Check for possible security issues with integration components from different cloud providers. - Assemble an expert team to ensure resilient security control development and avoid flaws/bugs i.e., develop a security test and evaluation plan.
4	***Implementation***	Cloud IT operations personnel are responsible for: - The security solution verification and testing. - The security solution rollout i.e., implementing the solution. - Initiating a security awareness and training program for personnel. - Updating implementation documentation as necessary. - Assembling a team of experts to ensure resilient security control development and avoid flaws/bugs i.e., developing a security test and evaluation plan.	- Revise and inspect the acceptance test results for any missing security components. - Inspect the security system and integration components and verify security performance. - Acquire security program certification and accreditation. ▪ Prior to certification and accreditation, the risk management results should be examined to determine if changes to the security program are required. ▪ *Certification:* based on the testing and evaluation plan, management should approve the security program. ▪ *Accreditation:* based on the certification results, the organization should make one of the following decisions: - *Accreditation is granted i.e., authorization to operate the program.* - *Conditional authorization to operate with some restrictions.* - *Deny authorization to operate the program.* ▪ If corrective actions are made to the security program, recertification and accreditation should be conducted. - Begin operation of the selected solution i.e., in a production environment.

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

5	***Operations and Maintenance***	Cloud IT operations personnel are responsible for: - Performance monitoring. - Operations support and maintenance. - Program modifications i.e., change management, service scalability, contract modifications, system updates or upgrades. - Ongoing security system assessment and proper training. - Security system documentation updates.	- Continuous monitoring of the security program and its performance in preventing threats. For example, adopting the security operations center proposed in [17]. - Configuration management and change control. For example, firewall access list add/delete entry, and enable secure telnet sessions to use SSH encrypted protocol on port 22. - Security system updates/upgrades and patch management i.e., antivirus and incident database updates, patch installation and development, patch testing, patch prioritization and scheduling, and test and approval and/or rollback. - Security control consistency and compliance monitoring. - Consolidated documentation and status reporting from all deployed security systems.
6	***Retirement and Deprovisioning***	Appropriate termination/disposal of a retired security system (physical, procedural and technical), is required to ensure the integrity of the security program. The cloud IT operations, information security, and risk management personnel are responsible for: - Revising and updating the cloud service level agreement and contract closeout. - Revising the policies for data preservation and retention. - Implementing the security program disposal/termination plan. - Conducting a disposal review. - Documenting lessons learned for future improvements of the SecSDLC.	- Verify that all cloud resources (e.g., applications, hardware, and virtual servers) have not been compromised. - Test the migration of security services, applications, and data to other service providers (if necessary). - Perform a complete backup of the security program services, documentation, and reports. - Ensure all cloud security services and equipment areterminated/disposed of in accordance with the security program disposal/termination plan. For instance, the data retention policy requires permanent purging of cloud critical data at the end of the contract unless there are business reasons or regulatory requirements for retaining the data in the cloud for a longer period.

Table 1 Thecloud security system development life cycle (SecSDLC) methodology tasks and measures.

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015
ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

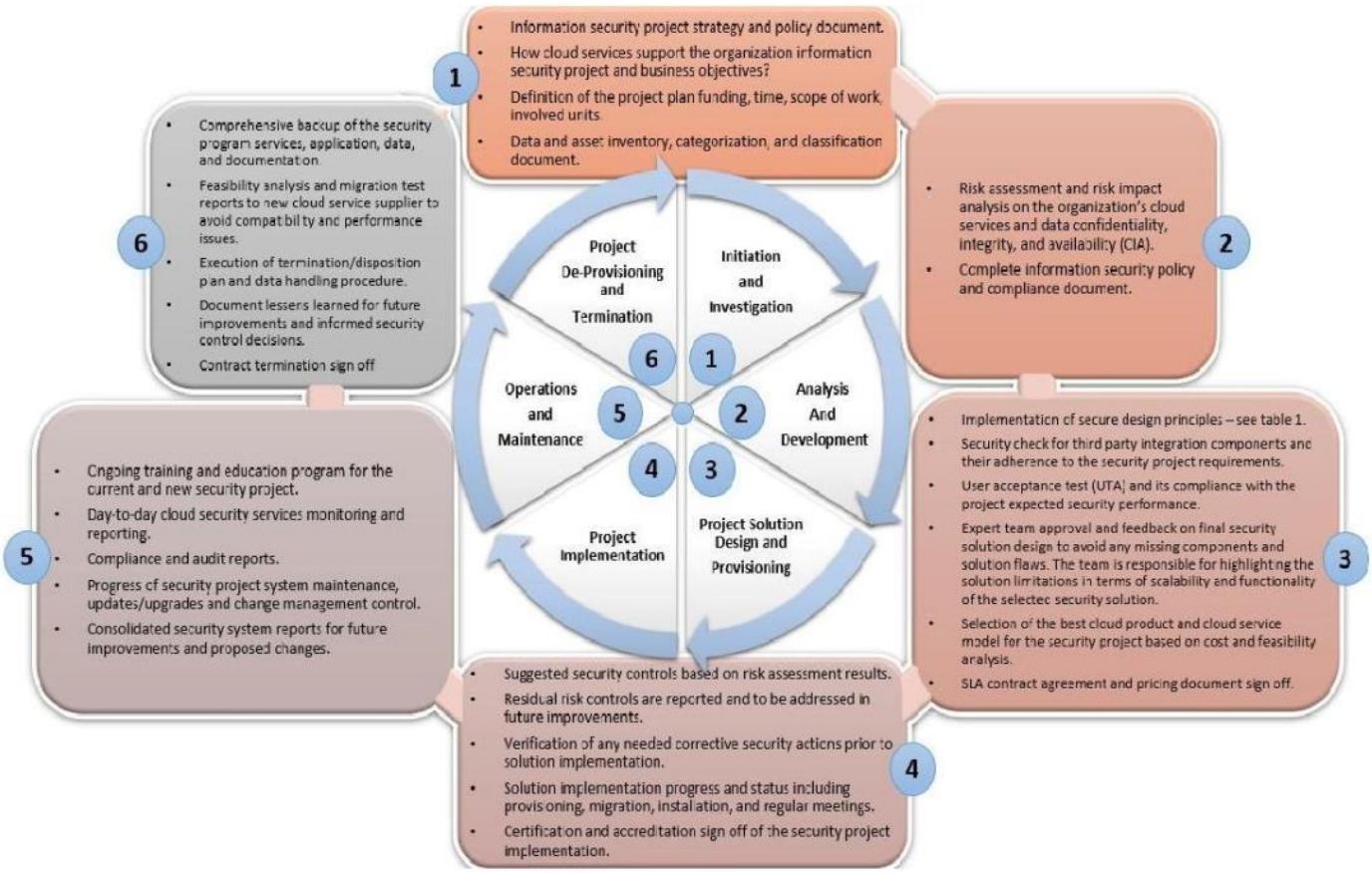


Figure 1 The SecSDLC methodology.

IV. Discussion

In this section, we discuss the advantages of the proposed SecSDLC approach, how it facilitates implementation of a cloud information security program, and how it satisfies the organization goals and requirements identified in Section I. The proposed SecSDLC first identifies the objectives, existing IT architecture and information security, and current policies and procedures of the organization. These form the start of the process to implement a cloud security program. The security plan must meet the business objectives, budget, time duration, and scope as defined by the organization during the initiation and investigation phase.

The SecSDLC not only provides a means of implementing effective security controls, but also an opportunity to refine and improve current security policies and information security training and education. The SecSDLC logical design phase translates the initial plan into a suitable security solution for implementation. This solution may include changes to improve security performance and achieve the desired outcomes. These changes are managed, communicated, tracked, and documented by the change management (CM) system.

The SecSDLC approach has a very positive impact on cloud security due to its comprehensive, iterative, and flexible phases. Information security solutions that are too secure may not be useful due to their complexity resulting in excessive resource consumption. The SecSDLC phases enable an organization to assess usability during each phase i.e., the feasibility of security features balanced with their usability. For example, public key infrastructure (PKI) is considered the most secure authentication technique, but many organisations do not employ PKI due to its complexity and alignment issues with usability models [25]. Information security and privacy experts should be employed in assessing the logical and physical

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015
ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

design i.e., Phase III, of the security program to ensure a suitable security solution. The SecSDLC provides a comprehensive approach to security program development that is secure, usable and efficient.

An important goal of a cloud information security program is to proactively detect, investigate, and respond to threats, confirm and manage identities, and prevent fraud and cyber crime in a cost-effective manner. The proposed SecSDLC is designed achieve this goal. Table 1 provides the guided steps cloud customers must perform during the phases of the security program life cycle discussed in Section III to satisfy the objectives and requirements of a cloud security program.

The proposed SecSDLC approach complements existing system development life cycles,yet it is tailored for cloud information security programs. It is the first to fit the cloud multi-tenancy model, i.e., the fundamental architecture of cloud computing services, and is meant to be used in conjunction with other cloud-specific measures [17], [31], [32]. Unlike traditional system development life cycles that employ the waterfall approach [34], the SecSDLC is an iterative process which enables agile and flexible changes during the design, development, and implementation of the security program. The on-demand provisioning of cloud services provides the flexibility to implement changes during all SecSDLC phases.

The SecSDLC promotes accountability though collaboration among the security program owners, developers, and operators. This enables diligent commitment, consensus, and rigorous analysis throughout the security program life cycle.

V. CONCLUSION

Implementing an effective cloud information security program is essential to address confidentiality, integrity, and availability requirements. The number and sophistication of malicious online threats is increasing. Therefore, it is critical that information security practitioners and researchers participate in solving cloud security issues and threats [35], [36], [37]. Recently, the Cloud Security Alliance (CSA) released version 3.0 of its cloud controls matrix (CCM) that contains a number of baseline controls adjustedfor cloud computing services and mapped to industry standards, regulations and frameworks, such as NIST, PCI DSS, HIPAA and COBIT [16]. Cloud organizations are advised to carefully review and include these controls in the SecSDLC logical and physical designs.

Cloud applications and services undergo constant changes and feature additions. Thus, cloud organizations must be proactive in ensuring that the associated security issues are appropriately addressed in the existing security program. Cloud service changes can significantly affect this program. Therefore, the goal of the proposed cloud SecSDLC approach is to design and implement an effective and agilecloud information security program that can quickly adapt to changes. This approach will not only simplify the process of implementing a successful security program, but also increase the likelihood of fulfilling cloud customer and service provider security and compliance requirements. In addition, it provides researchers with a methodology to focus on specific security problems throughout the life cycle of a cloud security program.

The proposed SecSDLC extends the traditional SDLC approach by incorporating cloud specific security concerns. The aim is to allow organizations that have or wish to migrate to the cloud to appropriately design and implement an information security program. The SecSDLC approach includes six phases, initiation and investigation, requirements analysis, development and provisioning, implementation, operation and maintenance, and deprovisioning and retirement. These phases provide for collaboration between IT managers, business units, and information security experts, to rigorously design, develop, implement, and operate an information security program. The security program begins with an analysis using the readiness model in [38] to identify areas of concern that must be addressed during the program life cycle. The SecSDLC approach leverages the widely used and

accepted SDLC waterfall methodology [34] and the NIST system development life cycle [18]. It is iterative so that changes can easily be incorporated. Prior to initiating an information security program, it is advised that organizations have clear security policies and compliance requirements. In addition, an organization considering cloud services for information security should understand the technology, service models, and limitations of the service providers.

REFERENCES

[1]. Yildiz, M., Abawajy, J., Ercan, T., and Bernoth, A. (2009) 'A Layered Security Approach for Cloud Computing Infrastructure', *International Symposium on Pervasive Systems, Algorithms, and Networks*, *IEEE*, pp. 763-767, December.

[2]. Ahmad, R., and Janczewski L. (2011) Governance Life Cycle Framework for Managing Security in Public Cloud: From User Perspective, *International Confernce on Cloud Computing, IEEE,* pp. 372-379, July.

[3]. U. ISACA, (2010) "ISACA US IT Risk/Reward Barometer Survey," *The Information Systems Audit and Control Association* [online], http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/ISACA-US-IT-Risk-Reward-Barometer-Survey.aspx, March, (accessed 12-12-2014).

[4]. ISACA, and Cloud Security Alliance (2010) Cloud Computing: Business Benefits with Security, Governance, and Assurance

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

Persepectives, *ISACA and CSA* [online], http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx, March, (accessed 17-12-2014).

[5]. Hiroyuki, S., Kanai, A., and Tanimoto, S. (2010) 'A Cloud Trust Model in a Security Aware Cloud', *International Symposium on Applications and the Internet, IEEE/IPSJ*, pp. 121-124.

[6]. Sultan N. (2011) 'Reaching for the Cloud: How SMEs Can Manage', *International Journal of Information Management*, Vol. 31, No. 3, pp. 272-278.

[7]. Stinchcombe, N. (2009) Cloud Computing in the Spotlight, *Infosecurity Magazine* [online], http://www.infosecurity-magazine.com/view/4755/cloud-computing-in-the-spotlight/, October, (accessed 14-12-2014).

[8]. Chow, R., Golle, P., Jakobsson, M., Masuoka, R., et al. (2009) 'Controlling Data in the Cloud: Outsourcing Computation Without Outsourcing Control', *in Proceedings Workshop on Cloud Computing Security, ACM*, pp. 85-90, November.

[9]. Symantec Corporation Technical Report (2010) State of Enterprise Security, *Symantec Corporation* [online], http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf, (accessed 13-12-2014).

[10]. Fan, C. K., and Chen, T. C. (2012) 'The Risk Management Strategy of Applying Cloud Computing', *International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 9, pp. 18-27.

[11]. Kalyvas, J. R., Overly, M. R., and Karlyn, M. A. (2013) 'Cloud Computing: A Practical Framework for Managing Cloud Computing Risk—Part I', *Intellectual Property & Technology Law Journal*, Vol. 25, No. 4, pp. 7-18, March.

[12]. Lindner, M., McDonald, F., Conway, G., and Curry, E. (2011) 'Understanding Cloud Requirements-A Supply Chain Lifecycle Approach', *International Conference on Cloud Computing, GRIDs, and Virtualization, IARIA*, pp. 20-25.

[13]. Morin, J., Aubert, J., and Gateau, B. (2012) 'Towards Cloud Computing SLA Risk Management: Issues and Challenges', *International Conference on System Science, IEEE*, pp. 5509-5514. January.

[14]. Conway, G., and Curry, E. (2012) 'Managing Cloud Computing: A Life Cycle Approach', *International Conference on Cloud Computing and Services Science, CLOSER*, pp. 198-207, April.

[15]. Cleeff, A. V. (2010) 'A Risk Management Process for Consumers: the Next Step in Information Security', *in Proceedings Workshop on New Security Paradigms, ACM*, pp. 107-114, September.

[16]. Cloud Security Alliance Research (2013) Cloud Controls Matrix v3.0, *Cloud Security Alliance* [online], https://cloudsecurityalliance.org/research/ccm/, September, (accessed 19-12-2014).

[17]. Alruwaili, F. F., and Gulliver, T. A. (2014) 'SOCaaS: Security Operations Center as a Service for Cloud Computing Environments', *International Journal of Cloud Computing and Services Science*, Vol. 3, No. 2, pp. 87-96, April.

[18]. NIST Special Publication 800-64 (2008) Security Considerations in the System Development Life Cycle, *National Institute of Standards and Technology* [online], http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf, October, (accessed 28-11-2014).

[19]. Cloud Security Alliance (2013) Governance, Risk Management and Compliance (GRC) Stack, *Cloud Security Alliance* [online], http://www.cloudsecurityalliance.org/grcstack.html, March, (accessed 15-12-2014).

[20]. Breiter, G. and Behrendt, M. (2009) 'Life Cycle and Characteristics of Services in the World of Cloud Computing', *Journal of Research and Development, IBM*, Vol. 53, No. 4, pp.3:1-3:8, July.

[21]. Kao, T. C., Mao, C. H., Chang, C. Y., and Chang, K. C. (2012) 'Cloud SSDLC: Cloud Security Governance Deployment Framework in Secure System Development Life Cycle', *International Conference on Trust, Security and Privacy in Computing and Communications, IEEE*, pp. 1143-1148, June.

[22]. Jaeger, P. T., Lin, J., and Grimes, J. M. (2008) 'Cloud Computing and Information Policy: Computing in a Policy Cloud?' *Journal of Information Technology & Politics,* Vol. 5, No. 3, pp. 269-283, December.

[23]. Ferrer, A. J., Hernández, F., Tordsson, J., Elmroth, E., Ali-Eldin, A., et al. (2012) 'OPTIMIS: A Aolistic Approach to Cloud Service Provisioning', *on Future Generation Computer Systems, ELSEVIER*, Vol. 28, No. 1, pp. 66-77, January.

[24]. Cloud Security Alliance (2009) Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, *Cloud Security Alliance* [online], https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, pp. 1-76, December, (accessed 11-12-2014).

[25]. Law, E. L. C., Hvannberg, E. T., and Cockton, G. (2008) 'Maturing Usability: Quality in Software, Interaction and Value', *on Human Computer Ineraction, Springer Verlag London Limited*, pp. 287–317.

[26]. PCI (2013) Payment Card Industry (PCI), Data Security Standard V.3.0, *PCI security standards council* [online], https://www.pcisecuritystandards.org/security_standards/documents.php?category=standards, November, (accessed 19-12-2014).

[27]. Sarbanes-Oxley Act (2002) U.S. Securities and Exchange Commission, *SOX* [online], http://www.sec.gov/about/laws/soa2002.pdf, July, (accessed 16-12-2014).

[28]. National Institute of standards and technology (NIST) (2002) The federal information security management act (FISMA), *FISMA* [online], http://csrc.nist.gov/drivers/documents/FISMA-final.pdf, (accessed 25-11-2014).

[29]. HHS (1996) Protecting Personal Health Information in Research: Understanding the HIPPA Privacy Rule, *Department of Health and Human Services* [online], http://www.hhs.gov/ocr/privacy, (accessed 22-12-2014).

[30]. The American Institute of Certified Public Accountants (AICPA) (2010) Statement on Auditing Standards No.70, *AICPA* [online], http://www.aicpa.org, May, (accessed 21-12-2014).

[31]. Alruwaili, F. F., and Gulliver, T. A. (2014) 'Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services', *International Journal of Future Generation Distributed Systems,* Vol. 1, No. 2, September.

[32]. Alruwaili, F. F., and Gulliver, T. A. (2013) 'CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services', *International Journal of Latest Trends in Computing,* Vol. 4, No. 4, pp. 151-158, December.

[33]. U.S.-European Union (EU) (2009) The U.S.—EU Safe Harbor Framework, U.S. *Department of Commerce* [online], http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf, (accessed 23-12-2014).

[34]. Balaji, S., and Murugaiyan, M. S. (2012) 'Waterfall vs V-Model vs Agile: A Comparative Study on SDLC', *International Journal of Information Technology and Business Management*, Vol. 2, No. 1, pp. 26-30, June.

[35]. Cloud Security Alliance (2010) Top Threats to Cloud Computing, *Cloud Security Alliance* [online], https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March, (accessed 10-12-2014).

[36]. Pawar, P. S., Rajarajan, M., Nair, S. K., and Zisman, A. (2012) 'Trust model for optimized cloud service', *Trust Management IFIP Advances in Information and Communication Technology, Springer*, Vol. 374, pp. 97-112.

[37]. Kaufman, M. L. (2010) 'Can public-cloud security meet its unique challenges?', *Security and Privacy, IEEE*, Vol. 8, No. 4, pp. 55-57, 2010.

[38]. Alruwaili, F. F., and Gulliver, T. A. (2014) 'ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud

International Journal of Research in Computer and Communication Technology, Vol 4,Issue 2 ,February -2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

Computing Services', *International Journal of Future Generation Distributed Systems*, Vol. 4, No. 4, November.

BIOGRAPHY OF AUTHORS

Fahad F. Alruwaili is a faculty member at computer science department at University of Shaqra, Saudi Arabia. He works as information security and computer networks consultant with over twelve years of practical experience and research development. He earned his BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he achieved his MS degree in Computer, Information, and Network Security with first class honour from DePaul University, Chicago USA. In 2011, he received his second MS degree in Information Systems and Technology from Claremont Graduate University, Los Angeles USA with first class honour. He is currently working towards achieving Ph.D. degree in University of Victoria, the Department of Electrical and Computer Engineering, Canada. His research interests are in the technical and theoretical views of information security and data privacy.

T. Aaron Gulliver received the Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.

Chapter 9

EVS: A Cloud Services Information Security and Privacy Eligibility and Verification System

As published in *International Journal of Research in Computer and Communication Technology*,
December 2015

This article appeared in Vol. 4, Issue. 12, published by *International Journal of Research in Computer and Communication Technology, Copyrighted to © IJRCCT.ORG Publisher, India*.
The attached copy is furnished to the author for internal non-commercial research and education use, including for instructions of the authors institution and sharing with colleagues.
Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.
In most cases authors are permitted to post their version of the article to their personal websites or institutional repository. http://ijrcct.org/index.php/ojs

International Journal of Research in Computer and Communication Technology, Vol 4, Issue 12, December- 2015
ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

IJRCCT International Journal of Research in Computer and Communication Technology

EVS: A Cloud Services Information Security and Privacy Eligibility and Verification System

Fahad F. Alruwaili and T. Aaron Gulliver

Department of Electrical and Computer Engineering
University of Victoria,
P.O. Box 1700 STN CSC
Victoria, BC V8W 2Y2 Canada
{fruwaili,agullive}@ uvic.ca

***Abstract*—In recent years, cloud computing services have evolved as a new paradigm for delivering computing resources thatare dynamic and customizable, and providehigh performance. Many organizations are migrating their information technology (IT) systems to the cloud due to the technological and economic opportunities it provides. However, security and compliance concerns exist that can undermine confidence and trust in cloud service providers. To address these concerns, an eligibility and verification system (EVS) is proposed to improve confidence and trust in cloud service providers, and the cloud community as a whole. The EVS architecture is designed to verify the existence of information security, privacy, and compliance (ISPC) controls in cloud services. This is achieved viaseveral measures, i.e. real-time monitoring, physical verification, and an in-depth five domain ISPC control matrix. This system establishes a foundation for promoting transparent, trusted, and compliant cloud services.**

***Keywords*—Compliance Verification, Cloud Information Security, Eligibility System, Control Matrix, Information Privacy.**

I. INTRODUCTION

Cloud computing services are considered to be the next generation technology based on a distributed computing platform that enables on-demand and dynamic provisioning of information technology (IT) resources. These services are offered as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), and leverage virtualization and internet technologies.

The research of the first author was sponsored in part by the Research and Development team from Innovative Solutions Company, Riyadh, Saudi Arabia.

Cloud IT capabilities are delivered to customers using a pay as you use model i.e., cloud customers can purchase resources as required, enabling agile adaptation to new IT demands. Cloud resource delivery eliminates the burden of establishing an IT system with the associated infrastructure and personnel [1], [2].

Currently, cloud service providers guarantee the quality of their services according to service level agreements (SLAs). However, these SLAs lack the technical means of enforcing and verifying the information security, privacy, and compliance (ISPC) required by customers and regulatory bodies [1]. The consequences of not begin compliant with ISPC internal policies and external regulations could be disastrous for both cloud service providers and customers [2]. The effects range from lost reputation, customer trust and confidence, to lawsuits and financial penalties. Thus, organizations wanting to migrate to the cloud have significant responsibilities when selecting a cloud service provider. The responsibilities are even greater for cloud service providers to ensure compliance with customer ISPC requirements.

Having control of cloud services allows providers to abstract the ISPC control management for their customers. Typically, the degree of control that customers have if they rent public cloud services is minimal [3]. Cloud customers can have more control over private cloud services, but there are other aspects to cloud control. For example, the location of cloud data and services can greatly impact data security and legal concerns [4]. In addition, it may be unrealistic to use public cloud services if the data is subject to legal restrictions and ISPC requirements unless cloud providers can furnish compliant and certified services. The many challenges for cloud providers in adapting ISPC requirements to acloud architecture necessitate new security

International Journal of Research in Computer and Communication Technology, Vol 4, Issue 12, December- 2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

models and frameworks. In this paper, a system is presented which can verify and monitor compliance with these requirements.

II. Customer Motivation and Requirements

Cloud computing has emerged as a cost-effective means of obtaining internet-enabled information technology (IT) services. Despite the benefits of cloud computing services, it is difficult to find the cloud provider best suited to customer requirements [5]. Many organizations have ISPC concerns, and this has created significant research and development in this area [6]. Addressing these concerns requires customer trust and confidence in cloud-enabled services, i.e. software, applications, and infrastructure.

It is often the case that organizations wanting to migrate to the public cloud do not adequately evaluate the information security and data privacy programs of potential cloud providers [7]. In addition, cloud service providers typically only make general terms and practices public, and are reluctant to disclose any details [8]. This has resulted in a significant increase in trusted third party audits [9]. Cloud customers and organizations wanting to adopt cloud services are advised to:

- *Select a cloud provider that exercise due diligence in adequately addressing ISPC requirements and concerns. Providers should also follow best cloud information security practices.*
- *Select a cloud provider that is transparent with regards to ISPC practices, including risk assessment, incident response, and security operations and monitoring.*
- *Select a cloud service provider that can implement security controls and practices tailored to cloud customers according to their ISPC requirements.*

To alleviate customer information security, privacy, and compliance (ISPC) concerns and assist them in selecting the most appropriate cloud service provider, a cloud ISPC eligibility and verification system (EVS) should be employed by a trusted third party to assess cloud providers based on their conformance to the ISPC criteria. Other criteria such as pricing and service features can be incorporated in this system, but the focus here is on ISPC as it is the key to cloud protection. The proposed system combines ISPC policies and controls based on best and widely accepted practices to assess the ISPC services of cloud service providers. Moreover, it allows organizations wanting to migrate their IT systems to the cloud to determine appropriate ISPC services prior to cloud provisioning.

III. Related Work

Despite the increasing acceptance of cloud services, many important security concerns remain unresolved or solved only partially [5]. One of these concerns is the verification and monitoring of ISPC compliance. The only approach related to that proposed in this paper is the automated security compliance tool (ASCT) presented by Zou et al. [10] to verify the compliance of cloud providers. This tool consists of three core components: data collection, verification engine, and user interface. However, it is limited to just access control to cloud services. In addition, no means of providing ISPC compliance are given such as ISPC controls, service linkage for real-time monitoring, historical performance, and compliance records, customer feedback, and compliance services.

Chen et al. [12] proposed an authentication-as-a-service (AaaS) architecture in order to protect sensitive customer information from the cloud provider and other customers. Two-factor authentication is employed based on AaaS generated tokens which provides some degree of trust and anonymity, but this approach is vulnerable to attacks such as distributed denial of service (DDoS). Supriya et al. [13] presented a trust management model to compare cloud service providers in terms of service quality and security. However, this approach is primarily intended to evaluate services and accessibility, and security is not considered in detail. In [13], a compliance solution was provided with location constraints mandated by regulatory authorities. However, only monitoring and tracing of cloud service IP addresses is employed, and these can easily be masked by an attacker, so additional security measures are needed.

IV. Eligibility Verification System (EVS) Overview

In this paper, the design science research (DSR) methodology for information systems is employed. This methodology employs a specific set of concepts and principles to develop IT solutions [14], [15]. The main DSR elements are summarized in Table 1. It begins with identifying the problem and setting the objectives, which are discussed in Section II. This is followed by designing, developing, and demonstrating the problem, which is presented as the EVS architecture in Section V.

In addition to the DSR methodology, the approach developed in [17] to verify and monitor the selected ISPC controls is employed. This allows potential cloud customers to determine if their acquired services are continuously compliant with the corresponding ISPC controls, which promotes cloud transparency and trust. Further, an ISPC

International Journal of Research in Computer and Communication Technology, Vol 4, Issue 12, December- 2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

control matrix is derived from the secure service level agreement (SecSLA) in [18] to assist in control evaluation. The SecSLA specifies the ISPC controls needed to satisfy cloud customer requirements. This is an extension of existing SLA agreements to include ISPC for cloud environments.

	GUIDELINE	DESCRIPTION
1	**Design**	The EVS system is a suitable model for determining provider eligibility and verifying cloud ISPC controls.
2	**Problem Relevance**	Despite the benefits of cloud computing services, it is difficult to find the cloud provider best suited to customer requirements [5]. Many organizations have ISPC concerns [6], and cloud service providers typically only make general terms and practices public, and are reluctant to disclose any details [8]. Thus trusted third party trusted audits are required [9]. The objective is to develop a solution which can be adopted by a trusted third party to verify the ISPC controls and cloud provider eligibility.
3	**Design Evaluation**	The EVS system is evaluated using an environment which reflects real world situations as a proof of concept.
4	**Contributions to Research**	The EVS system provides clear and significant contributions in the area of cloud ISPC.
5	**Research Rigor**	The proposed solution relies on rigorous information security methods and models acquired from the results in [17], [18].
6	**Design as a Search Process**	The search for an effective cloud eligibility and verification solution requires examining all available approaches to reach a solution.
7	**Research Communication**	The insights gained are disseminated to the cloud technology and management communities.

Table 1. Design Science Research (DSR)guidelines.

Incorporating the results in [16], [17] along with the DSR methodology makes EVS an effective tool for cloud customers to obtain information that is verifiable and accountable, and ensures that service providers comply with ISPC requirements. The information provided by the EVS supports the decision making processes for:

- *Cloud customers to select the most suitable service provider that is compliant with their ISPC requirements.*
- *Cloud providers to address missing ISPC components and obtain a competitive advantage in the cloud community.*

The EVS allows cloud customers to check the ability of service providers to comply with their ISPC requirements. The EVS user interface (UI) provides ISPC control tables so that potential customers can choose the most suitable controls. The tables are based on detailed ISPC control matrices. The advantages of the proposed approach are:

- *Potential customers can verify cloud service provider compliance with ISPC requirements. Informed and trusted decisions can be made based on EVS scores and results.*
- *Cloud service providers can verify their ISPC eligibility. This encourages cloud providers to become ISPC compliant which may provide a competitive advantage over other providers.*

The proposed EVS system encourages cloud service providers to provide trusted and compliant cloud services, and stay current in meeting the requirements of cloud customers. Typically, these requirements fall into one or more of the following areas:

- *Information security,*
- *Data privacy, and*
- *Compliance with internal policies and external regulatory requirements.*

A major reason for adopting the proposed EVS system is to achieve accountable, up to date, verifiable, transparent, and certified results. Thus, the system should be operated, managed, and maintained by a trusted third party. This third party is responsible for the EVS system results, and so is motivated to continuously verify the ISPC controls and closely monitor any changes to them.

V. THE CLOUD SECURITY SYSTEM DEVELOPMENT LIFE CYCLE

In this section, the eligibility and verification system (EVS) architecture is presented. The goal is to provide ISPC compliance verification capabilities as well as real-time monitoring. The EVS architecture is divided into several modules as shown in Figure 1 and described below.

International Journal of Research in Computer and Communication Technology, Vol 4, Issue 12, December- 2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

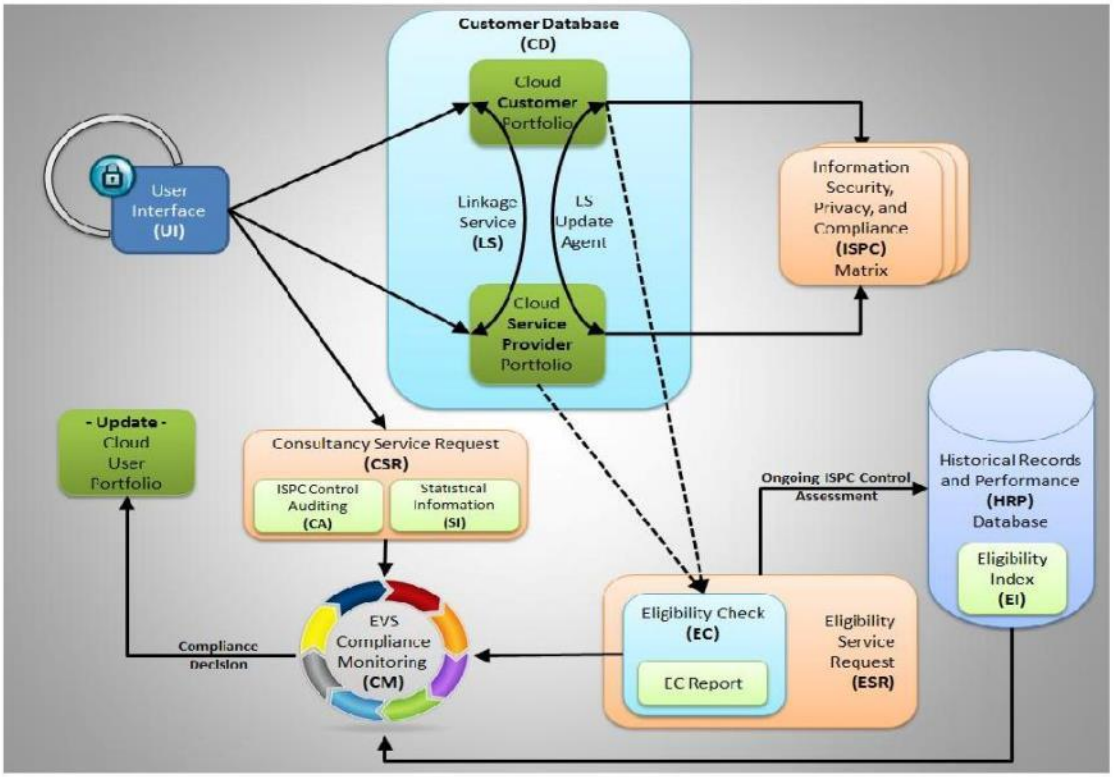


Figure 1. The eligibility and verification system (EVS) architecture.

A. *Customer-Provider Linkage Service (LS)*

The EVS linkage service (LS) is provided to customers and service providers to enable ISPC control verification and real-time updates. It begins when cloud customers select a cloud service provider and relevant services, or a cloud provider links its services to current customers. To establish the LS between a service provider and customer, one party initiates the request and the other validates and accepts the request. The LS function allows each customer to link their cloud services and monitor the associated ISPC compliance. The LS produces detailed information which can be compared with that provided by the eligibility index (EI) report discussed in Section V.C.

To terminate a link, the party that initiated the original LS request (link master) can execute a termination process. In addition, the connected party (request receiver), can revoke/terminate the link based on the EVS LS agreement. Figure 2 shows the LS establishment process. The same process is employed to terminate the link.

Consider an EVS system with C subscribed cloud customers. Once a linkage service is established, the compliance status of an associated ISPC control ls can be obtained by customer c from cloud service provider p. The status of an ISPC service can be compliant, non-compliant, or temporarily non-compliant, denoted as 1, 0, or -1, respectively. For customer c, the status of their controls over time can be expressed in a 2D matrix given by:

$$\begin{bmatrix} ls^c_{1,1} & \cdots & ls^c_{1,T} \\ \vdots & \ddots & \vdots \\ ls^c_{N,1} & \cdots & ls^c_{N,T} \end{bmatrix}$$

where n=1,..,N denotes a control, and t=1,…,T denotes time. If the status of a control is temporarily non-compliant, the time for a cloud provider to become compliant is specified in the agreement between the cloud customer and provider. If the status of a control becomes zero, the customer is

International Journal of Research in Computer and Communication Technology, Vol 4, Issue 12, December- 2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

informed that the relevant service is no longer compliant and further action is needed.

The real-time monitoring of ISPC controls and their compliance is governed by the LS update agent. This is typically done via service provider system logs and regular ISPC control assessments. The LS update agent is also responsible for coordinating updates among EVS system modules, i.e. historical records and performance (HRP) database, eligibility checks (ECs), and compliance monitoring (CM), to maintain up-to-date verification and eligibility data.

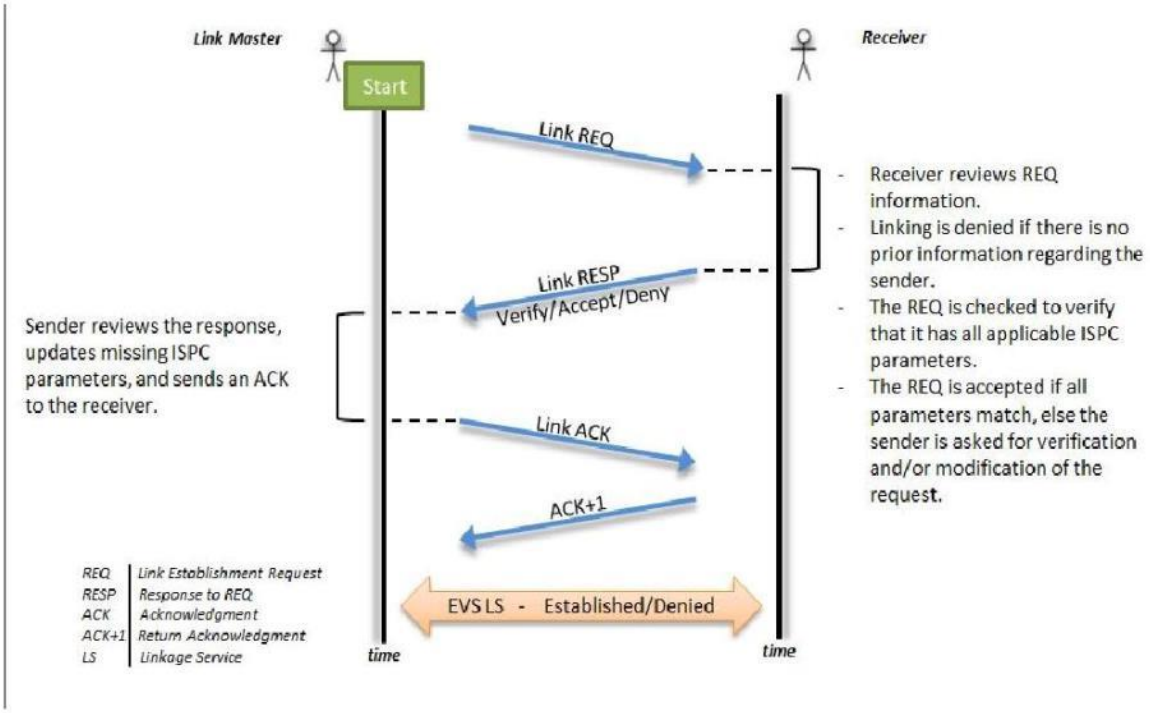


Figure 2. The EVS linkage process.

B. *Compliance Monitoring (CM)*

The compliance monitoring (CM) module operates as a dedicated session for each customer to monitor their ISPC requirements. The following are required to begin a session:

- *The customer must be subscribed to the EVS system.*
- *The customer must be linked to at least one cloud service provider.*
- *The service provider must exist in the EVS system.*
- *The customer must have selected the ISPC controls for the linked services.*

Cloud service providers that subscribe to the EVS system must keep their ISPC logs current to maintain their eligibility status (ES). The CM sets a schedule for cloud providers to update their logs. If an update is not received, the CM sends a message to immediately update the related ISPC records in order to remain compliant. Otherwise, the CM will change the status of the associated services that were previously compliant to temporary non-compliant until an update is received. If no update is received after a specified time period, the status of these services will be changed to non-compliant. The CM will also notify the affected parties, i.e. the linked cloud customers, and inform them once the cloud services return to compliant status.

As cloud customers can have different ISPC requirements, a cloud provider may be fully compliant with one customer but not with another. Therefore, CM consists of multiple monitoring sessions that correspond to the EVS services and linked cloud customers.

International Journal of Research in Computer and Communication Technology, Vol 4, Issue 12, December- 2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

Change requests are made to the CM by cloud customers to reflect new or revised ISPC requirements. The CM then notifies the linked cloud service providers of the changes. This should not affect the ES of the cloud providers until they have been approved by the providers and customers, and are in effect. The approval process is conducted by the EVS agent which is responsible for verifying the authenticity and existence of the changes, usually via ongoing ISPC control assessments, remote access, and if necessary site visits.

C. *Cloud Service Provider Historical Records and Performance (HRP) Database*

The historical records and performance (HRP) database contains information on service provider performance, customer feedback and satisfaction, pricing, third party auditor/assessor evaluations, and monitoring results. EVS customers have access to this database to obtain information on ISPC controls, location and pricing. This allows cloud customers to evaluate their current ISPC activities and refine their decisions to:

- *Adopt compliant cloud services.*
- *Improve the performance and functionality of their ISPC systems.*
- *Develop new services and products to gain a competitive advantage.*

The HRP database is updated based on ISPC changes, periodic monitoring, and ongoing ISPC control assessments. Cloud service provider changes that are not reported and/or reflected in the HRP database can lead to inaccurate conclusions as well as a loss of customer trust and confidence in EVS services. Therefore, this database is designed to ensure it contains accurate and current information. This is achieved by allowing cloud providers to send updates to the HRP at any time. The EVS agent verifies the authenticity and existence of all updates, after which they are added to the database and accessible by the relevant customers.

The ISPC eligibility index (EI) report provides verification of cloud provider conformance with ISPC requirements. The EI is part of the HRP database, but it does not contain detailed information on provider services and their compliance with control requirements (which is the function of the LS). However, it is useful for management who require an overview of the status of potential cloud providers. The EI report also allows customers to easily confirm that their cloud providers are compliant. Cloud service providers are scored on a scale, e.g. 0 to 10, according to their HRP records, where 10 indicates a very compliant and widely accepted service provider, 5 indicates partially compliant, and 0 denotes not compliant with the ISPC control requirements.

D. *The ISPC Control Matrix*

The ISPC control matrix contains information on the security, privacy, and compliance controls. It maps the ISPC contractual agreement to the set of controls to be applied to the relevant cloud services, i.e. storage, network infrastructure, platform, and applications. For example, a contractual requirement to implement data integrity entails that the intersection between cloud technology, data integrity controls, and cloud storage must be clearly defined. One security control to address this intersection is the implementation of cryptographic mechanisms and intrusion detection and prevention systems. This will protect the integrity of cloud data and alert involved parties of any unauthorized modifications to this data.

Cloud providers and customers use the ISPC control matrix to select the most appropriate ISPC controls. If an ISPC control is new and does not exist in the matrix, the EVS customer can request that a new entry be made. This matrix is based on the previously developed cloud ISPC cubic model [18], [21] that addresses information security and privacy in cloud service level agreements (SLAs). It covers the areas of confidentiality, integrity, availability, and privacy and their application to cloud service models, i.e. IaaS, PaaS, and SaaS. In this paper, this matrix is extended to include compliance so it has five domains to provide comprehensive ISPC coverage. These are confidentiality, integrity, availability, privacy, and compliance. ***Confidentiality*** measures are used to prevent unauthorized cloud information access and disclosure. For example, an organization should implement strong authentication methods such as two-factor authentication. User access can also be limited to only the information required to complete a certain task i.e. role based access control. An organization must implement ***Integrity*** measures to protect the authenticity of its critical assets from unauthorized modification, e.g. encrypting data. Since cloud resources are prone to attacks such as distributed denial of service (DDoS) that prevent customer access, ***Availability*** controls and service level agreements must be in place to address the issues of service interruption and maintenance. ***Privacy*** controls should also be identified to protect customer assets, e.g.a policy with a detailed explanation of what is acceptable (and also unacceptable) behavior to ensure security, privacy and compliance. Finally, ***Compliance*** controls are those terms and conditions identified in any applicable laws, regulations, contracts, strategies and policies, e.g. ISO27001, PCI DSS, and HIPAA. Customers want to ensure that cloud service providers continuous conform with all compliance requirements.

International Journal of Research in Computer and Communication Technology, Vol 4, Issue 12, December- 2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

E. EVS User Interface (UI)

The user interface (UI) provides a simple and practical means for customers to connect to the EVS system. The UI is typically a web portal. It is designed to allow EVS operators to optimize EVS processes and maximize usability. The UI serves both customers and subscribers, i.e. cloud service providers and cloud customers, but other organizations such as auditors and regulatory and legal entities can be given access. The EVS system should have a detailed service agreement with the operating entity i.e., trusted third party. Each subscribed customer should carefully review and accept this service agreement prior to selecting the EVS services. The following are available via the UI:

1. The EVS customer database (CD) allows customers to create a portfolio through a sign-up and validation process. This portfolio consists of the customer details and their preferred ISPC controls. The EVS agent is responsible for verifying portfolios and establishing their authenticity. Subscribed EVS customers receive updates of changes to their preferred ISPC controls.
2. An EVS consultancy service request (CSR) provides either a customer or EVS entity with the information required to review, evaluate, and accept consultancy agreements. These actions constitute a legal commitment, which protects both the EVS entity and customer. For instance, if an EVS entity provides a consultancy recommendation that fails to address the customer ISPC concerns, then it may be liable for any consequences. Conversely, if a cloud customer does not adopt the suggested EVS cloud solutions, the EVS entity will not be liable for any consequences. The CSR consist of:
    a. ISPC control auditing (CA) provided by independent trustees, i.e. accountants, legal entities, and ISPC auditors. An EVS customer is given access to the ISPC report of a cloud service provider only if it has an active relationship with the provider. Otherwise, the cloud service provider can choose not to disclose the audit report to potential customers.
    b. Statistical information (SI) retrieved from the HRP database to provide current and past information on cloud providers such as customer satisfaction, customer feedback, ISPC audit reports, ISPC availability, and ISPC control management.
    c. The eligibility check (EC) which is part of the EVS eligibility service as discussed below. Note that if requested, eligibility information on selected ISPC controls should be analyzed and sent to the customer.
    d. Consultancy reports which are digitally signed and sent to customers.
    e. Mandates for new ISPC controls, in which case additional advisory services can be delivered by the CSR. The CSR can act as a mediator between cloud customers and service providers to deliver the new controls. Once approved and implemented, these controls become new entries in the ISPC control matrix.

The UI should implement information security principles such as least privilege, defence in depth, and fail-safe stance in order to avoid or minimize security issues. The EVS designers should consider these principles early in the UI design and development process. This is critical as failure to adopt appropriate security principles can negatively impact customer confidence and trust [20].

F. EVS Services

The EVS system provides services to customers so they can verify the compliance of cloud service providers according to their ISPC requirements. The system also provides services to providers so they can verify their eligibility to satisfy ISPC requirements. These services are:

1. EVS eligibility service request (ESR)
    a. The cloud service provider selects the desired EVS services
        i. ISPC Eligibility Check (EC)
            1. The provider obtains a detailed description of the ISPC controls.
            2. The EVS agent verifies the existence and status of the ISPC controls.
            3. The EC provides a preliminary eligibility report.
            4. A comprehensive EC report is created, digitally signed and sent to the cloud provider.
            5. The report results are placed in the EVS, i.e. the HRP database, to ensure information is consistent and up-to-date.

        ii. Access to the HRP database
        Subscribed cloud providers have the ability to review their

International Journal of Research in Computer and Communication Technology, Vol 4, Issue 12, December- 2015 | ISSN (Online) 2278- 5841 ISSN (Print) 2320- 5156

historical records and performance information. If an error has been made, they can file a request to amend the database.

iii. Access to the EI

Subscribed cloud providers can obtain a summary of the EVS information. This consists of a ranked list of providers in terms of the existence and status of ISPC controls over a specified period of time, e.g. the past two years. The summary is sufficiently comprehensive for providers to make informed decisions on improving cloud services security and privacy compliance.

VI. Conclusion

Information security and data privacy violations are serious concerns, and it is important that procedures for avoiding and handling them are developed and adopted [19]. When cloud data falls under regulatory or compliance restrictions, organizations must know if a potential cloud service provider is compliant with their information, security, privacy and compliance (ISPC) requirements prior to cloud deployment and migration. Otherwise, information security, privacy, and regulatory requirements may be violated which can result in a loss of reputation and other serious consequences. Thus, it is expected that organizations will not select a cloud provider without verifying their compliance with the ISPC requirements.

In this paper, a reliable, trusted, and accountable ISPC eligibility and verification system (EVS) was presented. This system is based on a previously developed cloud trusted security model [16] to enable continuous monitoring and auditing by an accredited third party, i.e. 3PCAO or a third party cloud assessment organization. This enables the EVS system to assess the operation of all registered cloud service providers. Eligibility assessment results for cloud providers allow current and potential cloud customers to verify ISPC compliance and other criteria such as ISPC performance, pricing, and customer feedback and satisfaction. This will allow EVS customers, i.e. cloud providers and customers, to make strategic decisions based on current and historical ISPC information.

The EVS system determines ratings and eligibility based on log entries collected securely from the subscribed cloud service providers. EVS agents are used to verify the accuracy of the logs. This is done by remote access of system logs and/or site visits authorized under non-disclosure agreements. The system can be used to verify ISPC controls and compliant cloud services. However, to achieve this goal it must be accepted by the cloud community. The proposed system can also be used by cloud service providers to develop new ISPC initiatives to obtain a competitive advantage over other providers.

References

[1]. W. Itani, C. Ghali, A. Kayssi, and A. Chehab, "Reputation as a Service: A System for Ranking Service Providers in Cloud Systems," *Security, Privacy and Trust in Cloud Systems*,New York: Springer, pp. 375-406, January 2014.

[2]. M. Mehmejad, E. Toreini, and A. G. Bafghi, "Security Analyzing and Designing GUI with the Resources Model," *IEEE International Conference on Information Security and Cryptology*, pp. 29-36, September 2011.

[3]. G. Jones, "Penetrating the Cloud," *Network Security*, Vol. 2013, No. 2, pp. 5-7, February 2013.

[4]. K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud Forensics," *IFIP Advances in Information and Communication Technology Advances in Digital Forensics*, Vol. 361, New York: Springer, pp. 35-46, January 2011.

[5]. B. Hay, K. Nance, and M. Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing," *IEEE International Conference on System Sciences*, pp. 1-7, January 2011.

[6]. S. Wind, K. Turowski, J. Repschlager, and R Zarnekow, "Target Dimensions of Cloud Computing," *IEEE Conference on Commerce and Enterprise Computing*, pp. 231-235, September 2011.

[7]. R. Dutta and B Annappa, "Protection of Data in Unsecured Public Cloud Environment with Open, Vulnerable Networks Using Threshold-based Secret Sharing," *Network Protocols and Algorithms*, Vol. 6, No. 1, pp. 58-75, April 2014.

[8]. V. J. R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics. Amsterdam: Elsevier, 2011.

[9]. D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," *IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering* , pp. 1-10, May 2011.

[10]. D. Zou, W. Zhang, W. Qiang, G. Xiang, L. T. Yang, H. Jin, and K. Hu, "Design and Implementation of a Trusted Monitoring Framework for Cloud Platforms," *Future Generation Computer Systems*, Vol. 29, No. 8, pp. 2092-2102, October 2013.

[11]. K. W. Ullah, A. S. Ahmed, and J. Ylitalo, "Towards Building an Automated Security Compliance Tool for the Cloud," *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1587-1593, July 2013.

[12]. Y. Y. Chen, J. C. Lu, and J. K. Jan, "A Novel Design of Authentication-as-a-Services (AaaS) Architecture in Cloud Computing,"*Journal of Computers*, Vol. 24, No. 3, pp. 19-25, June 2013.

[13]. M. Supriya, K. Sangeeta, and G. K. Patra, "Comparison of Cloud Service Providers Based on Direct and Recommended Trust Rating," *IEEE International Conference on Electronics, Computing and Communication Technologies*, pp. 1-6, January 2013.

[14]. P. Massonet, S. Naqvi, C. Ponsard, J. Latanicki, B. Rochwerger, and M. Villari, "A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures," *IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum*, pp. 1510-1517, May 2011.

Chapter 10

Secure Cloud Migration to a Compliant Cloud: A Case Study

To be submitted to *International Journal of Research in Computer and Communication Technology*,
March 2016

Secure Migration to Compliant Cloud Services: A Case Study

Fahad F. Alruwaili and T. Aaron Gulliver

Department of Electrical and Computer Engineering
University of Victoria,
P.O. Box 1700 STN CSC
Victoria, BC V8W 2Y2 Canada
{fruwaili,agullive}@uvic.ca

***Abstract*—Migration to cloud computing technology is increasing in the financial sector to improve payment transactions, risk management, and business processes. This is occurring more rapidly in developed countries such as the USA, Canada, and the UK while cloud implementation in less developed countries such as Saudi Arabia is still emerging. Implementation of cloud technologies in the financial sector requires diligent decisions such as selecting the most suitable secure cloud deployment model, service level agreement, and cloud vendor. In this paper, cloud migration using an information security, privacy, and compliance (ISPC) readiness model is presented. Several types of cloud services are available, therefore evaluating the Saudi Arabia central bank migration readiness and selecting an appropriate vendor is critical, as this will have an impact on the requirements of stakeholders such as local banks. Cloud migration decisions are obtained by analyzing ISPC requirements considering the strategic initiatives of the organization. A case study involving the Saudi Arabian central bank agency is presented to demonstrate the implementation of the ISPC readiness model.**

***Keywords*—Readiness Assessment, Maturity Level, Information Security, Privacy, Compliance, Cloud Computing, Service Provider, Financial Payment Systems.**

I. INTRODUCTION

With the rapid advancement of the internet and data processing and storage capabilities, cloud computing has become a viable business model and computing paradigm. Cloud services enable powerful, scalable, cost-effective, on-demand, and efficient computing resources [1]. A variety of cloud computing service models such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) form the core cloud computing technologies. These service models are supported through different deployment models, i.e. public, private, community, and hybrid [2]. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3]. Further, cloud models are considered to have five essential characteristics, three service models, and four deployment models with different attributes compared to grid and distributed computing [4]. These attributes are described in Table 1. New service models are being developed such as storage as a service (STaaS), security and data protection as storage (SDPaaS), and security operations center as a service (SOCaaS) [5].

Many organizations are considering moving some or all of their information technology (IT) capabilities to the cloud due to the advantages of cloud technologies. However, migration decisions are not easily made, and can require significant time, resources, and expert personnel to assess the feasibility and readiness of an organization to make such a move [6]. This assessment considers decisions such as the selection of suitable cloud services and deployment models. If sensitive and business critical information is involved, a careful migration analysis must be conducted to identify the risks and benefits of cloud services [7].

The rapid growth in financial industry services and payment solutions requires greater agility to adopt and implement changes [8]. Cloud computing services enable organizations to quickly respond to new business requirements, and can be applied to financial applications and systems [8]. This paper considers the information security, privacy, and compliance (ISPC) requirements by presenting a case study that investigates the readiness and feasibility of the Saudi Arabian central bank migrating to cloud services. The focus is on the ISPC requirements that personnel should consider in the migration of payment systems to the cloud. In addition, commercial cloud solutions are investigated and considered for migration assessment. These solutions are (1) threat intelligence, i.e. evidence based knowledge including threat indicators, implications, and actionable advice about existing and emerging cyber security threats, and (2) eLearning systems, i.e. a system that administrates, documents, distributes, tracks, monitors, and reports user awareness assessments.

The research of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia and supported in part by Innovative Solutions Company, Riyadh, Saudi Arabia.

Cloud Deployment Models	Private	The cloud services are exclusively provisioned to a single organization. These services are managed by the organization or delegated to a third party.
	Community	The cloud services are provided to and shared by multiple organizations who have agreed to share similar concern, e.g. mission, policy, security requirements, and compliance.
	Public	The cloud services are provided for public use where multiple organizations can share cloud resources using a multi-tenancy model.
	Hybrid	The cloud services are provided as a combination of two or more of the above deployment models. These models retain their unique attributes, but are bound together by standardized or proprietary technology.
Cloud Service Models	Infrastructure as a Service (IaaS)	Cloud service provider provisioning of processing instances, storage, network, and other computing infrastructure resources.
	Platform as a Service (PaaS)	Cloud service provider provisioning of middleware, programming tools, operating systems, and other tools.
	Software as a Service (SaaS)	Cloud service provider provisioning of their deployed cloud applications.

Table 1. Cloud deployment and service models.

II. Related Work

Computing security is a major concern of organizations and government agencies considering migrating IT resources, e.g. email services, business process management, threat intelligence, security operations, training and awareness, and applications, to the cloud [9]. Migrating to the cloud can provide benefits such as flexibility and scalable on-demand IT services [10]. Further, the cost of IT operations and maintenance can be significantly reduced. However, there are few case studies that investigate the migration of IT capabilities to the cloud [11]. Moreover, the implications of cloud services from an enterprise and business perspective have not been adequately examined [12].

Hosseini et al. [13] identified several potential benefits in moving to the cloud. These benefits were viewed from a managerial perspective such as improved employee and customer satisfaction, opportunities to develop new applications, and reduced operational costs. Understanding these benefits and their associated risks are far from straightforward, so they introduced a conceptual framework to assist organizations in determining the cost, suitability and impact of adopting cloud services. However, ISPC requirements and readiness assessment were not addressed even though information security and privacy is a major challenge when migrating services to the cloud [14]. Many security experts believe that organizations hosting their data and applications on the internet and/or public cloud are quite vulnerable to threats and cybercrime [15]. Therefore, understanding the potential benefits and drawbacks of cloud services and assessing organization readiness is essential [14].

In [16], a forensic readiness model based on cloud capabilities was presented. This model allows cloud service providers to manage and deliver the data needed for digital forensic investigations. These investigations are important components of information security programs and security operations center activities. However, this model is limited to evaluating the readiness of data for forensic analysis. A number of techniques have been designed for readiness assessment, such as the tools and models described in the WEF 2009-2010 global information technology report [17] and the Waseda University world e-government ranking [18].

In [19], an ISPC readiness model was proposed to facilitate making decisions related to ISPC requirements. This model allows organizations to assess cloud risks based on the probability of threats occurring and their potential impact prior to and after migration. Both technical and non-technical issues were considered, i.e., payment technology, processes and procedures, and personnel awareness and readiness for cloud migration. In this case study, an implementation of the ISPC readiness model and ISPC cubic control [20] is presented for use in the migration readiness and decision-making process.

III. Case Study

A case study was conducted to examine the feasibility of cloud service implementation in the financial industry. The Saudi Arabia central bank governs all electronic bill payment transactions in the region. It is dedicated to streamlining electronic billing and payment systems operations while employing the highest information security standards and risk management principles. The agency currently employs a system developed in-house for executing payment transactions in accordance with policy requirements. While this system has provided adequate performance, there is an increasing need to provide customers with better real-time access and mobility. This initiative will enable the agency to develop new revenue streams and improve the efficiency of the payment system. Further, it will reduce costs and improve the management and operational control over financial transactions and reporting.

Personnel in the agency department of payment systems (DPS) and senior management knowledgeable of cloud computing service models and the associated risks were interviewed. This revealed many security, privacy, and compliance issues that should be addressed in the cloud migration plan. For simplicity, only the most important factors behind these issues are considered in this study.

This case study employs the cloud security concepts presented in [19], [20], [22], to address actual ISPC concerns associated with migrating a financial payment system to the

cloud. The methodology adopted and research motivation will first be presented, followed by the analysis of ISPC readiness for informed decision making. This is based on recent experience with the Saudi Arabia central bank and its ISPC readiness assessment. Further, the implementation and evaluation of commercial cloud security services, i.e. threat intelligence and phishing awareness services are considered. For clarity, only critical controls in the ISPC readiness model are discussed.

Overview of the Financial Agency

The Saudi Arabia central bank monitors and regulates all payment transactions in the country. It has been in existence for more than a decade regulating and monitoring payment transactions through multiple electronic payment systems such as real-time settlement system, bank transactions, and point of sale systems. The DPS is housed in three buildings and has approximately 530 personnel in diverse areas such as marketing, customer support, project management, application development, operations, information security, and risk management. The agency has developed three distinct payment products. The first presents payment transactions and settlements to process, monitor and regulate payments between government agencies and local banks. The second promotes cashless payments by increasing the number of point-of-sale (POS) locations. It also connects all ATMs nationwide with local and international banks and billers. The third system enables online payments between customers and billers, e.g. government agencies, transportation services, and educational, financial and insurance institutions.

The DPS systems are operated and supported by the financial agency. These systems consist of a complex collection of network architectures, servers, and desktop computers with dedicated wide area network (WAN) connections and high-speed internet connectivity. The agency has made a significant investment to establish the three payment products by procuring the necessary consultants and engineers, hardware, and software.

The Existing DPS

The three payment systems were developed nearly twenty years ago and require significant ongoing investments in software and hardware upgrades and maintenance. Increasing costs have made it difficult to stay within budget so that now the continuity and maintenance of the payment systems is a concern. For example, peak demand during month end payroll and special events, e.g. national holidays, results in system utilization near 70%, which is a critical level considering system scalability and performance. Further, there is an urgent need to redevelop the first payment system due to compatibility issues. This has been identified as a barrier to the strategic movement to a unified and integrated payment system.

DPS Challenges

DPS personnel are contemplating adopting cloud computing technology to reduce costs, minimize risks, improve the delivery and quality of payment systems, and address current problems. Newer technologies such as cloud services are cost effective due to their on-demand availability and pay per use services. Cloud services have other advantages such as scalability and accessibility from anywhere using any computing device. In addition, physical infrastructure including data center facilities, cabling, and servers can be eliminated or reduced significantly. However, while there are many benefits there are also challenges including the selection of a secure cloud deployment model.

As stated previously, cloud computing services can be categorized as one of three deployment models which differ in terms of purpose, complexity, capabilities and costs [24]. For example, a private deployment model is appropriate when the goal is to maximize and/or optimize the use of existing in-house resources, improve data privacy, and reduce costs [25]. A public deployment model is more suitable if remote access to non-sensitive tools, e.g. advanced learning tools, must be provided in a cost-effective manner [26]. DPS personnel have determined that the chosen strategy should consider the system architecture separately from other criteria such as mission, availability, and applications, as well as data criticality, sensitivity, confidentiality, integrity, privacy, and availability. Further, consultants have been employed to assess migration readiness and assist in the decision-making process. Based on these results, the following decision controls have been identified.

- **Organization Mission and Vision:** The DPS tends to be reactive to information security and privacy incidents instead of being predictive or even proactive. DPS personnel agree that clear objectives are essential in adopting and implementing an effective information security program [23]. Further, if the mission is not adequately defined, an organization will have difficulty securing its information and enforcing ISPC policies [27]. Therefore, the business and operations processes should be strategically aligned for cloud migration.
- **Confidentiality:** A key concern when considering the adoption of cloud technology is confidentiality. DPS personnel require effective end-to-end confidentiality measures without any degradation in service functionality. As the cloud services will be executing payment systems, data encryption is essential. This includes ensuring that all payment transactions are initiated from trusted parties. Further, financial messages between parties and authentication and cardholder information should be encrypted.

  Confidentiality depends on six essential controls:

  - *Antivirus:* There should be an online and up to date antivirus monitoring system to prevent virus and malware attacks.
  - *Authentication:* All data must be protection from unauthenticated users, and proper authentication mechanisms should be in place.
  - *Backup:* At regular intervals, online backup should be used to prevent data loss. DPS

policy requires a reliable backup mechanism, e.g. full backups, daily incremental backups, and real-time backups.

- *Disaster recovery:* A recovery system should be in place in case of data corruption.
- *Encryption*: Data encryption should be employed to protect the data.
- *Updates:* All applications should have automatic updating.
-

- **Integrity:** A critical component of information security is implementing controls to ensure data accuracy and consistency. It is required that integrity controls are implemented and continuously monitored across all payment systems. Therefore, a cloud service provider must provide adequate data integrity controls such as continuous monitoring and secure hash functions, e.g. the use of a hash-based message authentication code (HMAC) with secure hash algorithm 1 (SHA-1).
- **Availability:** It is essential that payment services always be available [28]. Thus, the cloud services should be available and accessible by all stakeholders 24/7/365, i.e. customers, banks, and billers. This is critical during peak load periods such as when monthly payroll transactions are executed. DPS personnel believe that current availability issues, e.g. downtime and lack of technical and customer support, can be resolved by adopting cloud technology.
- **Training, Awareness, and Education:** To deal with changes in cloud services and security, continuous training, awareness and education programs for DPS personnel must be provided. It is well-known that personnel are the greatest security threat with many incidents originating within the organization [29]. Thus, ongoing education and training programs are essential to achieving information security, privacy, and compliance program targets.
- **Management Support:** Senior DPS personnel are typically not information security experts. Thus, they must be provided with appropriate security awareness to understand the importance and criticality of ISPC. This will ensure proper support and resources for secure cloud migration.
- **Information Security, Privacy, and Compliance Policy:** The creation of an information security policy is a key step in determining the required direction and support for secure cloud migration. This policy identifies the critical assets of the payment systems and determines the control objectives and practices e.g. the acceptable use of cloud services to maintain security, privacy, and compliance. In addition, information security incident management is required to enforce compliance, protection, and recovery against malicious activities.

In the existing DPS systems, some networks are physically segregated from the internet to minimize cyber threats. However, this incurs additional expenses such as maintaining an isolated data center, cabling, communication lines, networking components, servers and workstations, licensing, and maintenance contracts. As a consequence, the services and infrastructure are not fully utilized as there are many situations when the equipment and personnel are idle, i.e. after business hours and during weekends. This is inefficient and costly, so DPS personnel are considering migration of these systems to the cloud. However, there are issues associated with ISPC requirements, for example, violations of ISPC requirements in a public cloud are more likely than with a private cloud. In either case, the use of cloud technologies can provide significant cost savings.

Due to the complexity of the security issues, it is difficult for DPS personnel to make a decision regarding the most appropriate secure cloud deployment model for the payment systems. Consequently, a detailed list of ISPC controls based on the approaches in [19], [20], [22] was obtained and used by to assess the readiness for migrating to a secure cloud model. A summary of the main ISPC controls is presented in Table 2.

Research Methodology and Motivation

This paper presents a case study regarding the issues surrounding the migration of payment system to the cloud [30]. The selection of a secure cloud deployment model requires an understanding of multiple factors and criteria from diverse perspectives. Further, it should consider how DPS personnel select and implement a secure, private, and compliant cloud service, and which vendor should be chosen [31]. The motivation for this study is to address the information security, compliance, and risk management concerns of DPS personnel in migrating payment systems, including security programs such as security awareness and threat intelligence, to cloud technology.

IV. Readiness Assessment and Decision Methodology

In this study, the ISPC readiness model in [19] is used to provide a detailed analysis in order to select the most appropriate cloud environment. This model provides guidelines for evaluating the readiness of the agency to migrate to a secure, private, and compliant cloud technology. It provides the required steps to select an appropriate cloud deployment model. These are used by the agency to make an informed decision on the suitability of cloud technology for their payment systems. In particular, the ISPC model provides DPS personnel with analysis results to make informed decisions.

For ***data analysis***, DPS personnel must create a data catalog, data classification, data event. and report logs to identify past and emerging threats and risks facing the agency. Further, an evaluation of cloud risks to the financial sector, in particular to payment systems, is undertaken to determine cloud behavior against such risks and the response and recovery procedures employed.

For effective ***decision-making***, the ISPC model requires that DPS personnel perform regular reviews and updates to the risk control strategies. Further, they should address the risks associated with migrating to a cloud environment. Cloud risk assessment should be an integral part of the DPS enterprise risk management framework. If they are within the acceptable risk tolerance, then migration is feasible.

The ISPC flowchart [19] details the methodology for evaluating current requirements and selecting the applicable cloud technology. The five main components of the ISPC model are discussed in the following steps.

STEP 1: ISPC Cubic Model

The first step is to define the problem, determine the objectives and alternatives, and identify the important ISPC elements. The goal is to select a secure and applicable cloud technology. The cloud cubic model [20] was used as a mapping tool between ISPC controls, e.g. policies, attributes, and controls. It represents a 3D structure for identifying ISPC controls to ensure visibility. For simplicity and also the privacy of the agency, only the most important controls are summarized in Table 2.

	ID	Control Family	Sub ID	Sub Control	Example
Non-Technical Measures i.e., Strategy, Policy, Plan, procedure, and Guidelines	OMV	The Department of Payment Systems (DPS) Objectives, Mission, and Vision	ISS	***Information Security Strategy***	The development of a long-term e.g., 3-5 year, security objectives aligned with the financial agency business objectives. These objectives are based on cloud ISPC readiness assessment.
			ISMF	***Information Security Risk Management Framework***	Aligned with the agency enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, to determine the likelihood and impact of all identified cloud risks.
			ISG	***Information Security Governance***	The DPS leadership reviews the information security policy at planned intervals or as a result of changes to the financial agency to ensure continuing alignment with the cloud security strategy, effectiveness, accuracy, relevance, and applicability to ISPC requirements or regulatory compliance obligations.
			ISC	***Information Security Compliance***	Cloud auditing activities and plans focusing on payment data, systems access, and data boundary limitations shall be designed to minimize the risk of payment system disruption. Audit activities must be planned and agreed upon in advance by cloud stakeholders, i.e. the agency, customers, banks, and cloud service provider.
			MS	***Management Support***	The agency executive and line management shall take formal action to support cloud migration and operations of payment systems through clearly-documented direction and commitment, and shall ensure the action has been assigned.
	ISPC	Information Security, Privacy, and Compliance Policy	NS	***Network Security Policy***	Cloud network environments and virtual instances shall be designed and configured to restrict and monitor traffic between the trusted and untrusted agency connections, reviewed at regular intervals, supported by documented business justification for the use of all services, protocols, and ports allowed. Network architecture diagrams must also clearly identify risks and data flows that may have legal, statutory, and regulatory compliance impacts.
			AS	***Application Security Policy***	Payment applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with ISPC requirements and industry acceptable standards (e.g., OWASP for web applications).
			SS	***Server Security Policy***	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.

	ID	Control Family	Sub ID	Sub Control	Example
			AU	***Acceptable Use Policy***	DPS policies and procedures shall be established, and supporting payment processes and technical ISPC measures implemented, for defining allowances and conditions for permitting usage of agency-owned or managed user end-point devices (e.g., desktops, laptops, and mobile devices).
			ESP	***Email Security Policy***	In addition to the AU policy above, a detailed email security policy must be created to enforce cloud email Phishing, SPAM protection. Sensitive emails must always be encrypted. Email archiving must also be checked and review with cloud service provider.
			PPP	***Password Protection Policy***	Password policies, applicable to DPS systems shall be documented and enforced through ISPC technical controls on all agency's devices or devices approved for mobility usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.
			PCI	***PCI DSS Compliance Policy***	The agency must adhere to the minimum mandatory PCI DSS requirements that need to be applied to all staff in DPS and cloud service provider and other stakeholders tasked with handling credit and debit cards, credit and debit cards data, and their processing systems/services.
			BCP	***Contingency, Business Continuity, and Disaster Recovery Planning Policy***	The DPS shall establish a consistent and unified framework for business continuity and disaster recovery planning and documentation shall be adopted to ensure all business and payment continuity plans are consistent in addressing priorities for DPS payment system testing, maintenance, and ISPC requirements.
			TAP	***Training and Awareness Policy***	A security awareness training program shall be established for all DPS staff, contractors, third-party users, and employees of the agency and mandated when appropriate. All individuals with access to the agency payment systems and payment data shall receive appropriate awareness training and regular updates on the agency ISPC procedures, processes, and policies relating to their job function.
Technical Measures	C	**Confidentiality**	CC	***Cryptography Controls***	Cloud service providers shall demonstrate compliance with confidentiality requirements. For instance, preserving authorized restrictions on access and disclosure for DPS systems in the cloud. Further, DPS system classification should be implemented and monitored at regular intervals.
			ISC	***Information Sharing Controls***	The DPS should enable information sharing for decision support. Controls must enable only authorized DPS users with access restriction clearness.
			ISRC	***Information in a Shared Resource Controls***	The cloud multi-tenant agency owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that cloud service provider user access is appropriately segmented from other tenant users, based on the following considerations: • Established resource sharing policies and procedures, and • Isolation of DPS critical assets and/or sensitive user

ID	Control Family	Sub ID	Sub Control	Example
				data and sessions that mandate stronger internal controls and high levels of assurance.
		TMAC	***Transmission Medium Access Controls***	The DPS and cloud service provider must implement access control management on transmission medium used between DPS, cloud service providers and other connected stakeholders. Controls such as two-factor authentication, physical security monitoring, and login attempt monitoring.
		TCC	***Transmission Confidentiality Controls***	Encryption techniques must be used to protect transmissions of DPS systems and user authentication and other confidential information passed over the Internet or other public networks. In addition, the DPS and cloud service provider must apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and packet black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.
		DLD	***Data Leakage Controls***	The DPS and cloud service provider should implement security mechanisms to prevent data leakage e.g., data encryption, classification, and access log monitoring.
		SSC	***Storage Security Controls***	The DPS and cloud service provider should implement restrictive and monitored access controls to offline storage, backup data, systems, and media.
		VSC	***Virtualization (hypervisor) Security Controls***	Access to all hypervisor management functions or administrative accounts for DPS systems hosting virtualized systems shall be restricted to personnel based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, and firewalls). Moreover, data exchanged between hypervisor sessions should also be classified and protected.
I	**Integrity**	SFIIC	***Software, Firmware, and Information Integrity Controls***	The DPS should review cloud service provider's cryptographic mechanisms for the protection of integrity e.g., digital signatures are used to sign hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information.
		IIVC	***Information Input Validation Controls***	Cloud service provider and DPS shall inspect, account for, and correct data quality errors and risks inherited. Checking the valid syntax and semantics of DPS payment system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. The DPS should periodically check the cloud service provider's prescreening measures for inputs prior to passing to interpreters prevents the content from being interpreted and modified. DPS and cloud provider should perform input validation to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and injection attacks.
		CARC	***Change and Access Restriction Controls***	The DPS and cloud service provider must ensure changes to hardware, software, firmware component of DPS systems and their cloud services are restricted

ID	Control Family	Sub ID	Sub Control	Example
				to only authorized individuals and processes. These changes should be permitted through change management control.
		TIC	***Transmission Integrity Controls***	The communication path outside of or between DPS and cloud service provider's and connected stakeholders premises are exposed to the possibility of modification. Therefore, DPS and cloud provider should apply cryptographic hash functions e.g., applying digital signatures, checksums, and message authentication codes. Further, the use of digital signatures is applied to all traffic for which nonrepudiation.
A	**Availability**	AAC	***Accountability and Auditing Controls***	The DPS and cloud service provider should be able to audit DPS system events, time stamps, records retention, and provide digital signature receipts for nonrepudiation.
		TAC	***Transmission Availability Controls***	The communication path outside of or between DPS and cloud service provider's and connected stakeholders premises are exposed to exposed to the possibility of service interruption. Therefore, DPS and cloud provider should develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with DPS availability requirements (including recovery time objectives).
		RC	***Redundancy Controls***	The DPS should ensure that cloud service provider implements adequate redundancy controls across all levels of DPS systems, e.g. network, server, and capacity, which may also reduce the susceptibility to denial of service attacks.
		CPMC	***Capacity Provisioning and Monitoring Controls***	The DPS must ensure cloud service providers implements appropriate CPU, memory, hardware and software resources capacity monitoring to address any future or immediate scalability requirements.
		BRC	***Backup and Restoration Controls***	The DPS must conduct regular backups of user-level, system-level, and hardware-level of all DPS systems hosted in the cloud. The restoration backups should also be available when needed.
		DOSC	***Denial of Service (DoS) Controls***	The DPS must ensure cloud service provider protects against or limits the effects of denial of service attacks. Additionally, the cloud provider should employ protection devices to filter certain types of traffic and should be able to increased capacity and bandwidth per DPS request.
P	**Privacy**	PIIC	***Inventory of Personally Identifiable Information (PII) Controls***	The DPS and cloud service provider should take due care in updating the inventories by identifying and linking any data that create PII, i.e. social security numbers, addresses, and credit card information. Therefore, to reduce disclosure risks and PII sensitivity, the DPS and cloud service provider, where feasible and within the limits of cloud service provider technology, locates and removes specified PII and/or uses anonymization and de-identification techniques.
		PIRC	***Privacy Incident Response Controls***	The DPS must ensure cloud service provider implements a proper incident response technique and procedure to respond to privacy incidents. This includes automated controls for immediate response

ID	Control Family	Sub ID	Sub Control	Example
				e.g., email notifications for involved individuals on incident status and expected resolution time.
		PMAC	***Privacy Monitoring and Auditing Controls***	The DPS and cloud service provider should implement technology to audit the security, appropriate use, and loss of PII. Further, conducting regular assessment e.g., risk assessment, identifies and addresses gaps in privacy compliance and its implemented controls.
		DRC	***Data Retention Controls***	The DPS and cloud service provider should only retain PII for the purpose identified in the notice or by regulatory e.g., PCI DSS cardholder data retention period. Storage and archiving controls are used for DRC.
		SDDC	***Secure Disposal of Data Controls***	The DPS and cloud service provider should implement the secure disposal and complete removal controls of data from all cloud storage media, ensuring data is not recoverable by any computer forensic means.
	C	Compliance	CPCM	***Compliance by Policy and Clauses Monitoring Controls***	The DPS and cloud service provider should perform periodic review of ISPC policy document and ensure cloud service provider's adherence to its latest version. Self-assessment controls should be implemented to detect any deviation from ISPC mandates.
			CCM	***Compliance by Control Monitoring***	The DPS and cloud service provider should perform ISPC compliance checks on cloud components prior to the DPS cloud migration plan. Automated controls should be enforced to detect violation of compliance e.g., change of hypervisor encryption protocol triggers a violation to ISPC controls unless change request was permitted.
			SLA	***Compliance by Service Level Agreement (SLA) Monitoring Control***	Cloud service provider SLA monitoring logs should always be reviewed by DPS for SLA assurance. The control reveals service interruption, threats to cloud network availability, and any other evidence that support DPS in the case of SLA violation.
			LMR	***Logging, Monitoring, and Reporting***	The PCI DSS requirement # 10 requires DPS to track and monitor all access to network resources and cardholder data. The DPS should ensure proper change management, incident response, system performance, system security, and account management solutions are employed by cloud service provider.

Table 2. Summary of the Information Security, Privacy, and Compliance Controls

STEP 2: ISPC Control Assessment

The second step is to assess the current and desired state for the ISPC controls. The results from step one are carefully examined using the systems security engineering capability maturity model (SSE-CMM) [19], [21]. Table 3 represents the relative maturity on a scale from 0 to 5 prescribed based on the CMMI. An example of the final readiness assessment findings for the current and desired control states is shown in Tables 4 and 5, respectively. Table 5 indicates that DPS personnel would like to improve the current ISPC controls to a more managed/maturity state. In the next section, the feasibility of migrating DPS systems with either the current or desired ISPC readiness to migrate to the cloud is discussed.

Maturity Level	Maturity Definition	Explanation	Control Readiness
0	Non-Existent	Cloud ISPC control is neither implemented nor present.	Not Ready
1	Initial	Cloud ISPC control is present but partially implemented and not well documented.	Ad-hoc Readiness
2	Repeatable	Cloud ISPC control is present but inconsistently implemented and partially documented.	Reactive Readiness
3	Defined	Cloud ISPC control is present, fully implemented, and documented.	Proactive Readiness
4	Managed	Cloud ISPC control is present, fully implemented, and	Predictive Readiness

		documented. Performance metrics for each ISPC control is defined and communicated.	
5	**Optimized**	Cloud ISPC control is aligned with the agency business processes and continuously improving. The control performance metrics are measured and monitored.	**Optimized Readiness**

Table 3. Cloud ISPC Readiness Levels

Control	Current Readiness Level					
	0	1	2	3	4	5
Department of Payment Systems (DPS) Objectives, Mission, and Vision	2	1	1	0	0	0
Information Security, Privacy, and compliance Policy	0	2	2	0	0	0
Confidentiality	0	0	3	3	0	0
Integrity	0	0	4	0	0	0
Availability	0	0	1	3	0	0
Privacy	0	3	2	0	0	0
Compliance	0	0	1	3	0	0
Current Readiness	2	6	14	9	0	0

Table 4. Current ISPC Readiness

Control	Desired Readiness Level					
	0	1	2	3	4	5
Department of Payment Systems (DPS) Objectives, Mission, and Vision	0	0	0	4	0	0
Information Security, Privacy, and compliance Policy	0	0	0	4	0	0
Confidentiality	0	0	0	3	3	0
Integrity	0	0	0	1	3	0
Availability	0	0	0	0	4	0
Privacy	0	0	0	3	2	0
Compliance	0	0	0	1	3	0
Desired Readiness	0	0	0	16	15	0

Table 5. Desired ISPC Readiness

STEP 3: Cloud Feasibility Analysis

The third step is to determine if cloud services are feasible and applicable to the agency payment systems ISPC requirements. In addition, this step takes the assessment results obtained from the previous step to address not only the current state of ISPC factors but also the identified desired state as well. The feasibility analysis (FA) consists of two parts:

Technical feasibility

Technical controls and sub-controls in the DPS are addressed here in terms of cloud feasibility to maintain or improve the technical operations of the agency payment systems. The DPS were advised to consider the following points:

- Compatibility with the selected cloud service. For example, payment applications should be tested using private cloud deployment model and IaaS. The test results should indicate zero issues running payment applications on any IaaS cloud instance.
- Ensure adequate capacity is assigned to handle the implementation of current and desired ISPC controls and sub-controls.
- Resource documentation required for cloud migration and maintaining payment systems operations are noted during the study including migration timelines, manpower, and cloud facilities.
- Response plan to any issues reported during the migration and proposal for alternative and/or compensative solutions.

Non-Technical feasibility

In this part, the economic factors and associated strategies, frameworks, policies and procedures of payment systems are considered. The department of payment system ensured that the cost of ISPC migration was justified and migration conforms to ISPC policy requirements. Additionally, the department revised their ISPC policy reflect new changes such as the inclusion of the secure cloud service level agreement in support to the payment systems operational performance and availability.

STEP 4: Readiness for Migration

This last step is to compile all results from previous steps for the DPS decision-making. The main idea is to help organize previous results for appropriate migration decision. Further, DPS experts should develop a detailed migration plan or roadmap when selecting the most ISPC compliant cloud provider. The DPS was advised to:

- Obtain management support and commitment to DPS cloud migration, i.e. migration decision.
- Create, audit, and update the migration plan according to the decisions made.
- Review the migration plan and make sure they meet the agency strategic goals and objectives.
- Perform testing to detect unforeseen limitations, e.g. missing components, lack of resources and trained personnel, and compatibility issues.
- Create a list of secure and suitable cloud service providers, i.e. cloud service providers A, B, C, and D in Table 6. Note that these are actual service providers, but due to confidentiality their names cannot be disclosed.

Control Details				Cloud Service Provider Applicability and Feasibility			
ISPC Control	Control	Current Readiness Level	Desired Readiness Level	A	B	C	D
OMV	*Department of Payment Systems (DPS) Objectives, Mission, and Vision*						
ISS	Information Security Strategy	0	3	✓	✓	✓	✓
ISMF	Information Security Risk Management Framework	0	3	✓	X	X	✓
ISG	Information Security Governance	2	3	X	✓	X	X
ISC	Information Security Compliance	1	3	X	✓	X	X
ISPC	*Information Security, Privacy, and compliance Policy*						
NS	Network Security Policy	2	3	✓	✓	✓	✓
AS	Application Security Policy	1	3	✓	✓	✓	✓
PCI	PCI DSS Compliance Policy	2	3	X	✓	X	X
BCP	Contingency, Business Continuity, and Disaster Recovery Planning Policy	1	3	X	✓	X	X
C	*Confidentiality*						
CC	Cryptography Controls	3	4	✓	✓	✓	✓
ISC	Information Sharing Controls	3	4	✓	✓	✓	✓
ISRC	Information in a Shared Resource Controls	3	4	✓	✓	X	X
TMAC	Transmission Medium Access Controls	2	3	X	✓	✓	✓
TCC	Transmission Confidentiality Controls	2	3	✓	✓	✓	✓
VSC	Virtualization (hypervisor) Security Controls	2	3	✓	✓	✓	X
I	*Integrity*						
SFIIC	Software, Firmware, and Information Integrity Controls	2	4	✓	X	✓	X
IIVC	Information Input Validation Controls	2	4	X	X	X	✓
CARC	Change and Access Restriction Controls	2	4	✓	X	X	✓
TIC	Transmission Integrity Controls	2	3	X	X	X	X
A	*Availability*						
AAC	Accountability and Auditing Controls	2	4	X	X	✓	X
TAC	Transmission Availability Controls	3	4	✓	✓	X	✓
CPMC	Capacity Provisioning and Monitoring Controls	3	4	✓	✓	✓	✓
DOSC	Denial of Service (DoS) Controls	3	4	X	✓	✓	✓
P	*Privacy*						
PIIC	Inventory of Personally Identifiable Information (PII) Controls	2	4	X	✓	X	X
PIRC	Privacy Incident Response Controls	2	4	✓	✓	✓	X
PMAC	Privacy Monitoring and Auditing Controls	1	3	X	✓	X	✓
RDC	Data Retention Controls	1	3	✓	✓	✓	✓
SDDC	Secure Disposal of Data Controls	1	3	✓	✓	X	X
Com	*Compliance*						
CPCM	Compliance by Policy and Clauses Monitoring Controls	3	4	X	✓	✓	✓
CCM	Compliance by Control Monitoring	3	4	✓	✓	X	X

SLA	Compliance by Service Level Agreement (SLA) Monitoring Control	2	3	X	✓	✓	✓
LMR	Logging, Monitoring, and Reporting	3	4	✓	✓	✓	✓

Table 6. Department of Payment Systems (DPS) Migration Readiness

V. Results and Discussion

From the above tables, it is clear that the DPS personnel would like to migrate to cloud technology. This is evident from the feasibility analysis and migration readiness i.e., steps 3 and 4. In particular, they have decided on migrating to the most suitable and secure cloud service provider meeting their minimum requirements for obtaining a private cloud deployment, as cloud service provider B ranks first in terms of the feasibility analysis. Further, they are not favorable towards public or community cloud deployment as they fear that payment transactions data would violate the DPS ISPC policy and compliance requirements. For example, placing such data in the cloud would make it vulnerable to hacking attacks, data leakage, and loss confidentiality, in comparison to other cloud deployment models, i.e. private and hybrid. As mentioned earlier, the DPS personnel believe that their payment systems and the required resources such as software packages should be available as and when required, and hence, availability issues can be resolved when moving to the cloud. Further, even though cloud technology may be elastic, scalable, private, and available, if the confidentiality, integrity, and compliance were not adequately addressed, migration would not be advantageous. Therefore, the main controls with respect to selecting a secure cloud deployment model as determined by the DPS personnel were clear. The decisions may be different for financial sectors in different jurisdictions due the corresponding security, privacy, and compliance legislation.

Managerial Relevance

The results presented in this paper have some key conclusions for practitioners, which are as follows:

- Although significant technical aspects of cloud security were addressed, this piece of work attempted to present a managerial view related to a decision problem of choosing a secure, private, and compliant cloud deployment model. It was demonstrated using a case study approach, which would benefit the financial practitioners – especially the IT security and risk managers of financial establishments as they might be addressing such problems commonly.
- Second, it attempted to utilize our prior work i.e., ISPC readiness model, with detailed step-by-step approach, which should benefit the IT security and risk personnel to make informed decisions while undertaking such strategic initiative e.g., applying cloud technology to payment systems.
- Third, various control factors for making this strategic decision were identified from our proposed ISPC control matrix along with detailed discussion with DPS decision makers, who are experienced in their domain. Hence, these control factors can also be used by the security and risk practitioners in financial industry, while addressing similar decisions in their organization.

Implications of the Decision

From the case study, it is evident that the DPS decision makers are interested in adopting the most secure and compliant cloud technology i.e., cloud service provider 'B'. The next sub decision would be whether this cloud to be created hosted and maintained by the DPS IT personnel or should it be outsourced to a trusted third party. A study on this decision-making situation can be taken up in as part of the future study. The implications of such decisions on the stakeholders of the agency are as follows:

- ***DPS Staff***

  Since the agency has adequate network resources, staff can access the required cloud hosted applications from their current locations. This should increase the productivity and performance of DPS staff and enable mobility. Typically, security principles for remote authentication, authorization, filtering and monitoring are applied for remote access. It is recommended that these be combined with the principles of least privilege authority and multifactor authentication, i.e. use of something you have, something you know, and something you are.

- ***DPS IT Center Staff***

  Currently, DPS IT center staff handle maintenance requests such as upgrades, repairs, support, re-installation, and imaging. In addition, the chances of application software and hardware failure or corruption can be significantly reduced when migrating to the cloud. Moreover, the number of the DPS IT center staff would be reduced when managing day to day DPS operations. Whilst, these issues are reduced, other calls for customer and technical support might still continue as currently to maintain access changes and additional logins needed to create and modify accounts.

- ***Management***

  The agency management saw potential cost benefits when choosing private cloud technology for their financial systems. The cloud pay-per-use and on-demand high availability models allow for not only tremendous savings but also proper utilization of their software and applications i.e., payment systems. Such benefits eliminate unwanted costs in terms of perpetual licenses and upgrading fees of application software.

Further, the fees for hardware resources, deployment, and implementation are minimized. These cost benefits enable the management to effectively plan their financial investment and cost savings and other benefits in an easier form. However, there is an incurred investment at the beginning of adopting the cloud where the agency has to create the necessary mechanism to train their staff and connected customers for utilizing the new way of operating financials in the cloud – yet the end benefits are expected to outweigh the cost of operating and supporting current payment systems.

Decisions Confirmed

In this case study, some decisions have been made to gradually migrate to cloud services. One decision to move the DPS security awareness program to the cloud was based on the analysis of our ISPC model. The awareness service acquired, namely 'InfoShield', was a comprehensive cloud-based eLearning awareness solution recommended by our work. In addition to 'InfoShield', a product name 'PhishMe' was also acquired for detailed awareness assessment of staff against phishing attacks. Both products are cloud services i.e., software as a service (SaaS) cloud service model. Utilizing these products by DPS information security department, all staff will be able to receive scheduled emails containing unique links to their accounts in 'InfoShield' eLearning system and/or PhishMe system. Clicking on the received links enable the assessment sessions to start and go through series steps of questions and actions needed from each staff. Each action indicates an awareness value, for example, an employee entering and submitting his ID or password into the link indicates weak awareness level, and hence customized content against the particular weakness is delivered to him. The goal is to heighten the level of information security awareness to all staff, educate payment systems' technical, non-technical, and business users to better secure information, monitor staff awareness level, and deliver customized content as per user awareness results. We were successful at the first live scenario where phishing emails were sent to all DPS staff to measure their reaction and response to such attacks. The results were compiled after the scenario ended and as shown in Figure 1, 2, and 3, 17.4 % of the staff are susceptible to phishing attacks, and hence 49 employees need appropriate and immediate awareness training. These results are recorded to measure awareness improvements with the next scenario e.g., time spent on learning as shown in Figure 3. InfoShield eLearning and PhishMe solutions were acquired to comply with payment compliance industry - data security requirement i.e., PCI-DSS, for awareness training. PCI DSS requirement 12.6 [32] stipulates having a formal security awareness program in place. Typically, the agency is responsible for processing and monitoring all payment transactions in the country and thus must comply with PCI DSS security standard. In The decision made to move DPS awareness program to the cloud was part of the overall cloud migration plan initiative.

Threat intelligence is another DPS ISPC requirement that promotes proactive incident response and defense capability. Threat intelligence is a cloud security monitoring solution that provides evidence-based knowledge about emerging threats based on targeted industry e.g., financial sector, technology e.g., CISCO routers, and geography e.g., Middle East. The DPS personnel sought to have an improved response plan and defense readiness against any threats affecting payment systems. A decision was made to acquire Symantec DeepSight, a cloud-based subscription threat intelligence service. This service complies with multiple DPS ISPC policy requirements i.e., incident response and mitigation policy, proactive security awareness requirement, and information security risk management policy, and information security integration. The last DPS ISPC policy requirement i.e., integration of threat intelligence, was included for automating the actionable advice fetched from DeepSight to the existing security information event management (SIEM) solution, hence faster and proactive response procedure.

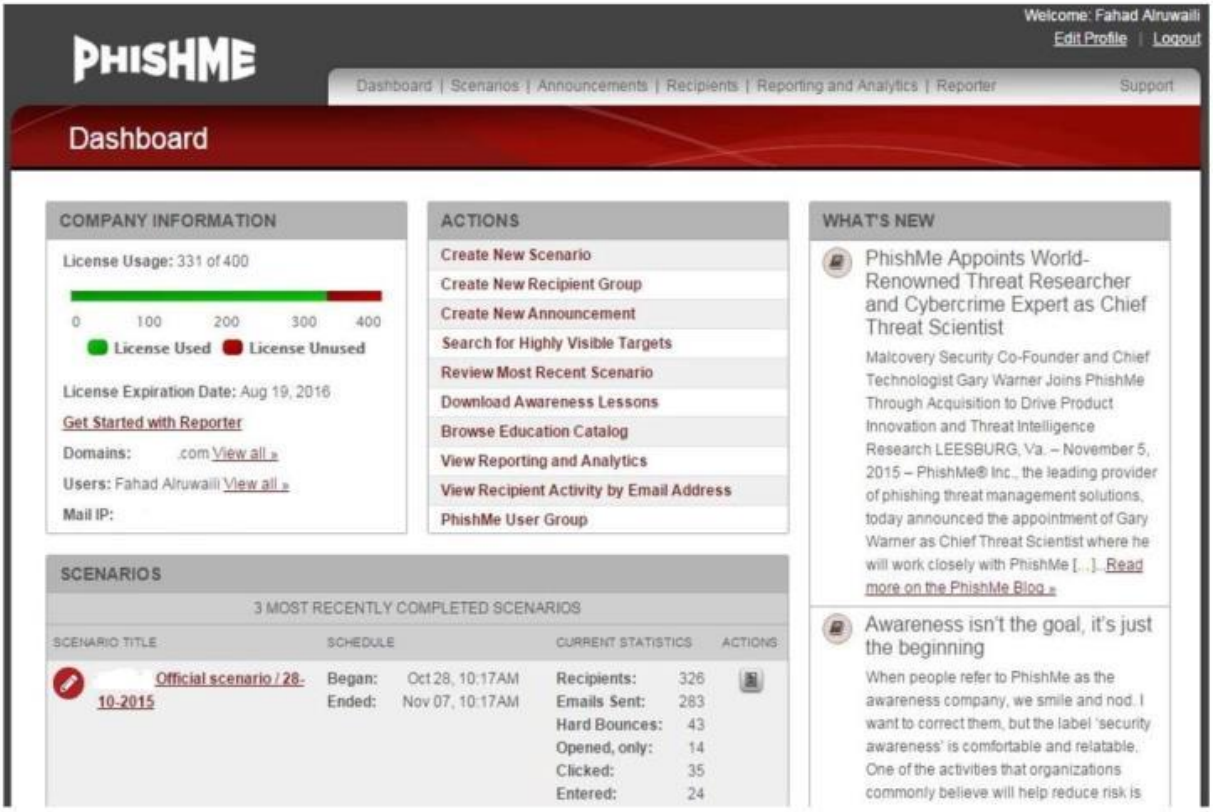


Figure 1. Phishing awareness administrative dashboard.

Figure 2. Phishing awareness response results.

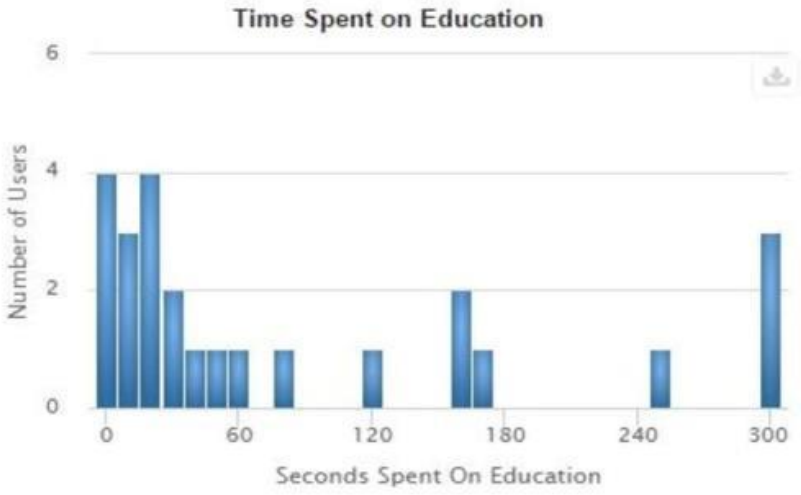


Figure 3. Time spent on awareness content.

VI. CONCLUSION

Cloud computing services are being considered by the financial sector around the world, but little has been done in M idle East countries such as Saudi Arabia. Further, existing studies on cloud adoption by the financial sector have not considered the architectures and models, or examined cloud services implementation. The decisions associated with the adoption of secure cloud services, such as the deployment models for implementing secure, private, and compliant cloud services have not been adequately examined. This paper provided a case study regarding migration to the cloud of the payment systems of the Saudi Arabian central bank using an ISPC readiness model. The ISPC requirements were used as decision factors using this model. The impact of migrating to the cloud, in particular the deployment of secure, private, and compliant cloud services, was examined and presented to DPS personnel. The results obtained led to the migration of DPS security, i.e. threat intelligence and security awareness, to the cloud through the adoption of InfoShield, PhishMe, and Symantec DeepSight.

REFERENCES

[1]. M. Jouini, A. B. Aissa, L. B. A. Rabai, and A. Mili, "Towards Quantitative Measures of Information Security: A Cloud Computing Case Study," *International Journal of Cyber-Security and Digital Forensics - Society of Digital Information and Wireless Communications*, Vol. 1, No. 3, pp. 248-262, 2012.

[2]. S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Elsevier Journal of Network and Computer Applications*, Vol. 34, No. 1, pp. 1-11, January 2011

[3]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology (NIST)*, http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, 2011. Last viewed (02-01-2016).

[4]. S. Hossain, "Cloud Computing Terms, Definitions, and Taxonomy," *Cloud Computing Service and Deployment Models: Layers and Management: Layers and Management*, October 2012.

[5]. F. F. Alruwaili and T. A. Gulliver, "SOCaaS: Security Operations Center as a Service for Cloud Computing Environments," *International Journal of Cloud Computing and Services Science*, Vol. 3, No. 2, pp. 87-96, April 2014.

[6]. R. Ranjan, R. Buyya, S. Nepal, and D. Georgakopulos, "A Note on Resource Orchestration for Cloud Computing," *Wiley Concurrency and Computation: Practice and Experience*, Vol. 27, No. 9, pp. 2370-2372, June 2015

[7]. A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, "Cloud Migration: A Case Study of Migrating an Enterprise it System to IaaS," *IEEE International Conference in Cloud Computing*, pp. 450-457, July 2010.

[8]. A. Shi, Y. Xia, and H. Zhan, "Applying Cloud Computing in Financial Service Industry," *IEEE International Conference in Intelligent Control and Information Processing*, pp. 579-583, August 2010.

[9]. C. Barron, H Yu, and J. Zhan, "Cloud Computing Security Case Studies and Research," *In Proceedings of the World Congress on Engineering*, Vol. 2, pp. 3-5, July 2013.

[10]. D. C. Wyld, "Moving to the Cloud: An Introduction to Cloud Computing in Government," *IBM Center for the Business of Government*, November 2009.

[11]. I. Sriram and A. Khajeh-Hosseini, "Research Agenda in Cloud Technologies," *ACM Symposium on Cloud Computing*, January 2010.

[12]. A. Khajeh-Hosseini, I. Sommerville, and I. Sriram, "Research Challenges for Enterprise Cloud Computing," *ACM Symposium on Cloud Computing*, January 2010.

[13]. A. K. Hosseini, D. Greenwood, J. W. Smith, and I. Sommerville, "The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in the Enterprise," *Wiley Journal of Software: Practice and Experience*, Vol. 42, No. 4, pp. 447-465, April 2012.

[14]. A. R. Kurdi, A. Taleb-Bendiab, M. Randles, and M. Taylor, "E-Government Information Systems and Cloud Computing (Readiness and Analysis)," *IEEE International Conference on Developments in E-systems Engineering*, pp. 404-409, December 2011.

[15]. B. Bailey, "Cloud Computing may Create New Venues for High-Tech Criminals," San Jose Mercury News, http://www.mercurynews.com/businessbreakingnews/ci_12812412?nclick_check=1, Septemeber 2009. Last viewed (13-01-2016).

[16]. G. Sibiya, T. Fogwill, H. S. Venter, and S. Ngobeni, "Digital Forensic Readiness in a Cloud Environment," *IEEE Conference on AFRICON*, pp. 1-5, September 2013.
[17]. S. Dutta and I. Mia, "ICT for Sustainability," *World Economic Forum on Global Information Technology Report 2009-2010*, 2010.
[18]. T. Obi, "Waseda University World e-Government Ranking," *Research report of the Waseda University Institute of e-Government*, http://www.waseda.jp/eng/news10/index.html, January 2010. Last viewed (11-01-2016).
[19]. F. F. Alruwaili and T. A. Gulliver, "ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services," *International Journal of Future Generation Distributed Systems*, Vol. 4, No. 4, November 2014.
[20]. F. F. Alruwaili and T. A. Gulliver, "SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services," *International Journal of Cloud Computing and Services Science*, Vol. 3, No. 4, August 2014.
[21]. ISO, and IEC, "Information Technology Systems Security Engineering—Capability Maturity Model (SSE-CMM, ISO/IEC 28127)," *International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC)*, 2002.
[22]. F. F. Alruwaili and T. A. Gulliver, "Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services," *International Journal of Future Generation Distributed Systems*,Vol. 1, No. 2, September 2014.
[23]. M. Al-Awadi and K. Renaud, "Success Factors in Information Security Implementation in Organizations," *International e-Society Conference International Association for Development of the Information Society*, pp. 169-176, July 2007.
[24]. N. Ramachandran, P. Sivaprakasam, G. Thangamani, and G. Anand, "Selecting a Suitable Cloud Computing Technology Deployment Model for an Academic Institute," *Campus-Wide Information Systems*, October 2014.
[25]. T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," *IEEE International Conference on Advanced Information Networking and Applications*, pp. 27-33, April 2010.
[26]. S. Stein, J. Ware, J. Laboy, and H. E. Schaffer, "Improving K-12 Pedagogy via a Cloud Designed for Education," *Elsevier International Journal of Information Management*, Vol. 33, No. 1, pp. 235-241, February 2013.
[27]. J. McKay, "Pitching the Policy: Implementing IT Security Policy through Awareness," *USA: SANS Institute*, http://www.giac.org/paper/gsec/3223/pitching-policy-implementing-security-policy-awareness/105199, July 2003. Last viewed (09-01-2016).
[28]. P. Pocatilu, F. Alecu, and M. Vetrici, "Measuring the Efficiency of Cloud Computing for e-Learning Systems," *WSEAS Transactions on Computers*, Vol. 9, No. 1, pp. 42-51, January 2010.
[29]. F. H. Katz, "The Effect of a University Information Security Survey on Instruction Methods in Information Security," *ACM Proceedings of the Annual Conference on Information Security Curriculum Development*, pp. 43-48, September 2005.
[30]. P. Baxter, and S. Jack, "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers", *The Qualitative Report*, Vol. 13 No. 4, pp. 544-559, 2008.
[31]. R. K. Yin, "Applications of Case Study Research," *Sage Publications India Private Ltd*, 3rd ed., June 2011.
[32]. M. Gorge, "Data Protection: Why are Organisations Still Missing the Point?," *Computer Fraud & Security*, Vol. 6, pp. 5-8, June 2008.

Fahad F. Alruwaili is a faculty member in the College of Computing, University of Shaqra, Saudi Arabia. He works as information security and risk management consultant with over twelve years of practical experience and research development. He received the BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he received the MS degree in Computer, Information, and Network Security with first class honours from DePaul University, Chicago, IL USA. In 2011, he received the MS degree in Information Systems and Technology with first class honours from Claremont Graduate University, Los Angeles, CA USA. He is currently a Ph.D. candidate in the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC Canada. His research interests are in the technical and theoretical views of information security and data privacy.

T. Aaron Gulliver received the Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.

Chapter 11

Conclusion and Future Research Directions

Summary

Current advancements have made cloud services attractive to customers and enterprises of all sizes. Today, large cloud service providers are not particularly interested in investing in cloud standardization. The cloud market is expanding and evolving very rapidly, before required standards and frameworks are established. In other words, the absence of widely accepted standards degrades information security, privacy, and compliance issues associated with cloud services. Failure to provide in depth cloud security frameworks to address the common security issues can lead to slow acceptance of the cloud. This case is even more critical to organizations handling sensitive information and services that must adhere to compliance requirements. Typically, these issues are related to the current settings of information security programs and their management by cloud service providers. In order to obtain comprehensive and effective security, privacy, and compliance measures, more robust models and frameworks are needed. The main focus of this research was to develop appropriate frameworks for assessing, monitoring, and enforcing the information security, privacy, and compliance of cloud systems. The research aims were achieved through the development of eight approaches to address cloud customer and service provider information security concerns. These approaches were presented in Chapters 2 to 9.

These approaches are devised to fit the cloud service multi-tenancy architecture which can be made universal and effective if adopted by cloud service providers and trusted third party assessment entities. They provide scalability which means that they can be expanded to include very large scale of computing nodes. For example, the work presented in Chapter 2 is heavily dependent on collaboration and scalability to provide robust cyber threat intelligence for current and new threats. They allow us to view cloud ISPC assessments and readiness from a novel perspective, and define the needed

requirements and components. In a sense, they tackle the lack of standardization in a conceptualized and generic way. Although, they have the merit of providing potential rewards in terms of accomplishing a more secure and compliant structure than what exists today, there are still implementation limitations due to the lack of support of current cloud computing technologies. Current cloud simulators are not flexible for implementing and integrating developed approaches in terms of, for instance, visualization and modelling of security operations and their strategies.

Finally, a case study was presented which shows how to implement and support cloud migration decision and readiness to the central bank of Saudi Arabia. The application of the work presented in this research, i.e. risk management, SecSLA, and ISPC readiness frameworks, are possible implementations to support the central bank DPS decision assessment to migrate to a suitable cloud service provider. It is a complex mission which requires collaborative efforts between DPS stakeholders and careful evaluation of payment systems criticality versus feasibility to cloud migration. The integrated frameworks form a roadmap for making an effective and informed migration decision. As a result, a cloud based eLearning management solution was acquired to replace the in-house awareness and training system. Further, a cloud threat intelligence service was selected to promote proactive and strategic defenses against current and emerging cyber security threats. The decision to migrate the central bank payment system is pending.

Future Research Directions

This dissertation discussed initial work to provide comprehensive and practical security and privacy frameworks. The implementation and testing tasks are part of the future plans towards conceptualization of a cloud ISPC. Some of the developed frameworks have already been identified as strategic opportunities for cloud managed security service providers. Cloud computing is in its early stages and hence the development of applicable tools for support and assessment of the frameworks capabilities is required.

The main aspect of this research provides a foundation for further study into the standardization aspects of ISPC to ultimately promote transparent and trusted cloud services. The proposed approaches and scenarios have seen in cloud computing, but require further attention to gain short and long term strategic advantages in both ISPC efficiency and effectiveness. These challenging areas include:

- Leveraging the full potential of CCIPS, SecSLA, Risk Management, SecSDLC, and ISPC Readiness frameworks. These frameworks can be massively scalable and powerful, and hence require rigorous testing to perform adequately in different scenarios.
- The interoperability and applicability of the frameworks presented has not been entirely tested, except for the case study which resulted in potential benefits to the central bank of Saudi Arabia. Consequently, we are building a prototype of the EVS system and comparing cloud customer requirements and characteristics against applicable cloud providers. This work will be used to develop business case to provide real-time compliance monitoring for current and prospective cloud customers.
- Further investigation to support the decision-making process regarding customer and provider readiness and ability to provide effective ISPC requirements is required. Continuous enhancements of cloud security technologies, standards, and policies are also challenges ahead.

The results obtained from the case study address some of those ISPC challenges, including:

- Identification requirements and characteristics of IT systems and resources planned for migration and their criticality and sensitivity.
- Security and privacy concerns with regards to migration of classified and/or critical systems to the cloud.
- Selection of the most suitable and compliant cloud service provider.
- Decision-making regarding cloud provider feasibility to meet customer ISPC technical and non-technical requirements.
- Customer readiness for migration.

For these issues in the central bank of Saudi Arabia, the implementation of the proposed models was suggested to a conduct comprehensive readiness assessment in an effort to best match the central bank organizational capabilities and their ISPC requirements with current cloud offerings. During the study, constraints were detected that could potentially delay the decision making and/or data collection processes; some of which could impact the reliability of end results. Some of these are:

- Absence of a clearly defined and communicated information security strategy and framework.
- Lack of or outdated documentation, e.g. internal or external audits, outdated infrastructure and network logical and physical designs, and acceptable use policies.
- Undefined and/or out of date risk tolerance which guides the organization willingness to accept/tolerate risks associated with cloud services.
- Conflict or lack of interest among key stakeholders.
- Lack of adequate knowledge or awareness of cloud services and cloud cyber threats.

The results presented in this dissertation can be optimized and applied as a next step to further test cloud ISPC models. This can be done with practical scenarios for the suggested models where thorough testing for both efficiency and effectiveness can be better understood.

Given the potential savings and computing agility that cloud services offer, this dissertation provides a way forward for cloud implementation. However, there is a need for proper support of resources and usage of cloud computing in order to turn this vision into reality and promote cloud trustworthiness and its adoption. With current ISPC issues, the benefits of considering the proposed approaches, is the support of industry for both assessment and cloud ISPC standardization is worth the effort.

Bibliography

[1]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, **Vol. 53, No. 4**, pp. 50-58, 2010.

[2]. M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and A. Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," *IEEE Internet Computing*, **Vol. 13, No. 5**, pp. 10-13, 2009.

[3]. J. W. Rittinghouse, and J. F. Ransome, "Cloud Computing: Implementation, Management, and Security," *CRC Press*, 2009.

[4]. L. Wang, G. V. Laszewski, A. Younge, X. He, M. Kunze, J. Tao, and C. Fu, "Cloud Computing: a Perspective Study," *Springer New Generation Computing*, **Vol. 28, No. 2**, pp. 137-146. 2010.

[5]. L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, "Scientific Cloud Computing: Early Definition and Experience," *IEEE High Performance Computing and Communications*, **Vol. 8**, pp. 825-830, September 2008.

[6]. W. Voorsluys, J. Broberg, and R. Buyya, "Introduction to Cloud Computing," *Cloud Computing: Principles and Paradigms*, pp. 3-37, 2011.

[7]. S. Long, "Virtual Machine Graphics Acceleration Deployment Guide," *VMWare Technical*, 2013.

[8]. A. J. Younge, J. P. Walters, S Crago, and G. C. Fox, "Evaluating GPU Passthrough in Xen for High Performance Cloud Computing," *IEEE International Symposium on Parallel and Distributed Processing*, pp. 852-859, May 2014.

[9]. D. Quick, and K. K. R. Choo, "Google Drive: Forensic Analysis of Data Remnants," *Elsevier Journal of Network and Computer Applications*, **Vol. 40**, pp. 179-193, 2014.

[10]. N. Xue, and L. Chang, "Design Tradeoffs in Applying CAS to File System Backed by Amazon-S3," *Applied Mechanics and Materials*, **Vol. 543**, pp. 3423-3426, 2014.

[11]. W. T. Tsai, X. Sun, and J. Balasooriya, "Service-Oriented Cloud Computing Architecture," *IEEE International Conference on Next Generations Information Technology*, pp. 684-689, April 2010.

[12]. P. Mell, and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology*, **Vol. 53, No. 6**, pp. 50, 2009.

[13]. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-Art and Research Challenges," *Journal of Internet Services and Applications*, **Vo. 1, No. 1**, pp. 7-18, 2010.

[14]. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE Transactions on Services Computing*, **Vol. 5, No. 2**, pp. 220-232, 2010.

[15]. Sun Microsystems, Inc., "Building Customer Trust in Cloud Computing with Transparent Security," https://www.sun.com/offers/details/sun_transparency.xml, Nov. 2009, Last viewed (02-09-2016).

[16]. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, **Vol. 16, No. 1**, pp. 69-73, 2012.

[17]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," *ACM Conference on Computer and Communications Security*, pp. 598-609, October 2007.

[18]. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," *USENIX Conference on Hot Topics in Operating Systems*, pp. 1-6, may 2007.

[19]. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," *Cryptology ePrintArchive*, Report 2008/186, http://eprint.iacr.org, 2008, Last viewed (02-12-2016).

[20]. K. SO, "Cloud Computing Security Issues and Challenges," *International Journal of Computer Networks*, pp.11-14, 2011.

[21]. D. Chen, and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *IEEE International Conference on Computer Science and Electronics Engineering*, **Vol. 1, pp. 647-651**, March 2012.

[22]. "Top Threats to Cloud Computing," Cloud Security Alliance, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010, Last viewed (02-23-2016).

[23]. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0," Cloud Security Alliance, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011, Last viewed (12-20-2015).

[24]. R. Krutz, and R. Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing," *John Wiley & Sons*, pp. 3, 2010.

[25]. S. Pearson, and G. Yee, "Privacy and Security for Cloud Computing," *Springer Science & Business Media*, pp. 130, 2012.

[26]. K. Beckers, S. Faßbender, and H. Schmidt, "An Integrated Method for Pattern-based Elicitation of Legal Requirements Applied to a Cloud Computing Example," *IEEE International Conference on Availability, Reliability and Security*, pp. 463-472, August 2012.

[27]. R. Samani, J. Reavis, and B. Honan, "CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security," *Syngress*, 2014.

[28]. Cloud Security Alliance, "Privacy Level Agreement," CSA, https://cloudsecurityalliance.org/research/pla/#_resources, December 2014, Last viewed (02-02-2016).

[29]. G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems," *NIST special publication 800.30*, 2002.

[30]. T. Finne, "A Conceptual Framework for Information Security Management," *Elsevier Computers & Security*, **Vol. 17**, pp. 303–307, 1998.

[31]. D.W. Straub, "Deterring Computer Abuse: The Effectiveness of Deterrent Countermeasures in the Computer Security Environment," *Dissertation, Indiana University Graduate School of Business*, 1986.

[32]. A. Blumstein, J. Cohen, & D. Nagin, "Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates," *National Academy of Sciences Panel on Research on Deterrence and Incapacitation Effects on Assembly of Behavioural and Social Sciences (US)* , pp. 431, 1978.

[33]. Cloud Security Alliance Research, "Cloud Controls Matrix v3.0," Cloud Security Alliance, https://cloudsecurityalliance.org/research/ccm/, September 2013.

[34]. J. Show, "Information Security in Practice from an Activity-Theoretic Perspective," *The Annual Security Conference*, pp. 241-248, April 2007.

[35]. Y. Engestrom, "Activity Theory and Individual and Social Transformation," *Perspectives on Activity Theory*, pp. 19-38, 1999.

[36]. P. Massonet, S. Naqvi, C. Ponsard, J. Latanicki, B. Rochwerger, and M. Villari, "A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures," *IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum*, pp. 1510-1517, May 2011.

[37]. A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," MIS Quarterly, pp. 75-105, March 2004.

[38]. R. K. Yin (2013). *Applications of Case Study Research*, 3rd ed., Sage Publications India Private Limited, Retrieved from https://books.google.com/.

[39]. P. Baxter and S. Jack, "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers," *The Qualitative Report*, **Vol. 13, No. 4**, pp. 544-559, 2008.