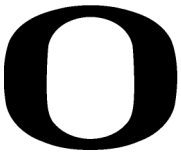
Presented to the Interdisciplinary Studies Program:



UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Identifying Cloud Computing Security Risks

CAPSTONE REPORT

Paul S. Wooley
Network Analyst
Tyco Electronics

University of Oregon
Applied Information
Management
Program

February 2011

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger
Senior Academic Director, AIM Program

Identifying Cloud Computing Security Risks

Paul Wooley

Tyco Electronics

Abstract

Cloud computing services including Infrastructure as a Service promise potential cost savings for businesses by offering remote, scalable computing resources. However attractive these services are, they pose significant security risks to customer applications and data beyond what is expected using traditional on-premises architecture. This paper identifies three basic types of threats related to the IaaS layer and eight kinds of attacks. These are aligned within the CIA model as a way to determine security risk.

Keywords: cloud computing, C.I.A. security, Infrastructure as a Service (IaaS), virtual computing, attack surface

Table of Contents

List of Figures and Tables

Introduction to the Literature Review

Problem Area

What is cloud computing. "Cloud Computing is associated with a new paradigm for the provision [sic] of computing infrastructure" (Vaquero, Rodero-Merino, Caceres, & Lindner, 2008, p. 50) that migrates computing services provided by on-premises datacenters to remote systems located on the Internet. "Cloud computing represents a shift away from computing as a product that is purchased, to computing as a service that is delivered to consumers over the Internet from large-scale data centers – or 'clouds'" (Khajeh-Hosseini, Sommerville, & Sriram, 2010, p. 1). This remote service "… can be defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as a services over the Internet (Furht & Escalante, 2010, p. 3).

Cloud computing services are offered in three different forms; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Vaquero et al., 2008). In the Infrastructure as a Service mode, customers are allocated computing resources in order to run virtual machines consisting of operating systems, and applications (Chudnov, 2010). The best known example of IaaS is Amazon.com's Elastic Compute Cloud service (Conry-Murray, 2009). In the Platform as a Service model, the consumer is allowed to write applications that run on the service provider's specific environment. "A well-known example is the Google Apps Engine" (Vaquero et al., 2008, p. 51). The third delivery model, Software as a Service, provides the consumer with typical software applications that run over the Internet. "The Google Docs programs are an example, including a word processor, a spreadsheet, and a tool for creating PowerPoint-like presentations" (Hayes, 2008, p. 10).

Cloud computing as a way to lower costs. Cloud computing is a technology promoted as a way to lower an organization's data processing costs by outsourcing the underlying infrastructure (Hinchcliffe, 2009). Much of the cost savings generated comes from downsizing the staff no longer required to maintain on-premises systems (Khajeh-Hosseini, Greenwood, & Sommerville, 2010). Wang, Ren, Lou, and Li (2010) state that:

> … storing data remotely in a cloud in a flexible on-demand manner brings appealing benefits: relief of the burden of storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, personnel maintenance, and so on. (p. 19)

Chudnov (2010) notes that in a search to lower costs while still delivering services to end users, " … free or low prices can make offloading service hosting into the cloud a worthwhile move" (p. 33). Khajeh-Hosseini, Greenwood, et al. (2010) study the potential for cost savings realized by migrating on-premises infrastructure to cloud computing. They also conclude that "cloud computing could potentially eliminate many support-related issues since there would be no physical infrastructure to maintain" (p. 7).

Cloud computing and security risk. "On the other hand, along with these benefits, Cloud Computing also raises severe concerns especially regarding the security level provided by such a concept" (Jensen, Gruschka, Schwenk, & Iacono, 2009, p. 109). Migrating to a cloud computing infrastructure poses security risks to an organization's data (Mather, Kumaraswamy, & Latif, 2009). "One of the biggest user concerns about Cloud Computing is its security, as naturally with any emerging Internet technology" (Furht & Escalante, 2010, p. 24). Mather et al.

(2009) outline six primary concerns about security when talking about cloud computing: data-in-transit, data-at-rest, processing of data, including multitenancy, data lineage, data provenance, and data remanence (magnetization). Data in transit should be encrypted in order to preserve confidentiality. Data at rest is also subject to compromise when it is not encrypted (Mather et al., 2009).

Purpose

The purpose of this study is to identify security risks inherent in the cloud computing service known as Infrastructure as a Service (IaaS) (Armbrust et al., 2010; Mell & Grance, 2010). Once identified, risks are aligned with the C.I.A. security model (Gilliam, 2004).

Cloud IaaS is the capability provided to the consumer to deploy operating systems and applications on self provisioned remote computer resources that include processors, storage, and networks (Mell & Grance, 2010). An example of an IaaS offering is Amazon's Elastic Compute Cloud (EC2) (Jensen et al., 2009). The essential characteristic of IaaS offerings is that the consumer "delivers virtual machine images to the IaaS provider, instead of programs, and the machines can contain whatever the developers want" (Viega, 2009, p. 106).

In order to complete this task, the study is organized into two stages. First, a pre-selected framework of security objectives is presented (Gilliam, 2004). This set of security objectives, known as C.I.A., refers to three concepts which include: (a) confidentiality, described as the assurance that data is be kept secret, (b) integrity, which refers to the inability to alter or destroy data by accident or malfeasance, and (c) availability, which is the ability to access that data whenever it is needed (Gilliam, 2004). The C.I.A. security model is chosen because it is popular (Canal, 2005) and is described in detail by Stoneburner (2001) in fulfilling the National Institute

of Standards and Technology's "… statutory responsibilities under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996" (p. 1). Stoneburner (2001) states that the goal of these security objectives is to "enable an organization to meet all of its mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners and customers" (p. 2). The second task is to identify reported security risks in the literature in IaaS cloud computing and to align these against the set of security objectives. Cloud computing services are described by the "SPI" framework (Mather et al., 2009). These three offerings include: Software as a service (SaaS) Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (Armbrust et al., 2010). The study is concerned with the IaaS model because it represents the lowest level of cloud computing service available and offers the highest level of control over the operating system, data, and applications the customer chooses to run on the system (Rittinghouse & Ransome, 2010).

Infrastructure as a Service (IaaS) is the repackaging of on-premises, dedicated computer infrastructure including servers, and networks into services the consumer rents in the form of virtualized systems with dedicated processing power, storage, and network access (Furht & Escalante, 2010). "Usually, the service is billed on a monthly basis, just like a utility company bills customers. The customer is charged only for resources consumed" (Rittinghouse & Ransome, 2010, p. 35). The primary purported advantage to the infrastructure as a service model is that the "customers maintain ownership and management of their application(s) while off-loading hosting operations and infrastructure management to the IaaS provider" (Rittinghouse & Ransome, 2010, p. 35). In addition, the cloud service provider has the ability to partition, assign, and scale the size computing resources to match the consumers' needs dynamically (Vaquero et al., 2008).

Audience

The goal of this study is to inform information system managers how to apply the C.I.A. security framework to the security risks that cloud computing introduces into the data processing workflow. This literature review is intended for an audience that includes an organization's "Chief Information Officer (CIO), Chief Information Security Officer (CISO) and/or Chief Security Officer (CSO), Chief Risk Officer (CRO), and Chief Privacy Officer (CPO)" (Westby & Allen, 2007, p. 6). The expectation is that these individuals can use the study to identify the security risks (Gilliam, 2004) of the Infrastructure as a Service model (Armbrust et al., 2010). The literature review is intended for information mangers responsible for identifying and acting upon security risks associated with the use of the Infrastructure as a Service cloud computing services available. It provides a list of those security risks, associated with (IaaS), in order to inform the individuals responsible for managing such systems within their organizations.

Outcome

This literature review provides a list of security risks reported in the selected literature that are associated with the Infrastructure as a Service (IaaS) cloud computing service offerings. Identified security risks are aligned within the C.I.A. security objectives model, in order to inform the individuals responsible for managing cloud computing systems within their organizations.

Significance

Armbrust, et al. (2010) suggest that Cloud Computing has the potential to transform a large part of the information technology industry by fulfilling the dream of computing as a utility. However, many questions about the security risks of cloud computing remain; Talbot (2010) states that:

> Cloud computing actually poses several separate but related security risks. Not only could stored data be stolen by hackers or lost to breakdowns, but a cloud provider might mishandle data - or be forced to give it up in response to a subpoena. (p. 38)

This study provides important information for organizations that are using cloud computing resources now or plan to in the future. Gilliam (2004) maintains that corporate survival is contingent on information technology risk management. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level (Stoneburner, Goguen, & Feringa, 2002). Unfortunately, as noted by Mather et al. (2009), risk management of cloud computing is not a mature science. "Risk management in cloud computing is an evolving area, and standards are being debated by the community" (p. 279).

Kaufman (2009) explains that the "industry itself should establish coherent and effective policy and governance to identify and implement proper security methods" (p. 63) for creating and maintaining a security regime that supports the C.I.A. security objectives. Kaufman goes on further to suggest that cloud service providers make available encryption, access controls, and scheduled backup to safeguard all data. Unfortunately, Mather et al. (2009) note that "given the current lack of agreed upon standards across providers, it is unlikely that customer requirements

for mitigating controls to manage risk translate into the control framework of cloud service providers" (p. 279).

Delimitations

Topic scope. This study is limited in scope to identifying security risks by applying the C.I.A. security objectives (Gilliam, 2004) to cloud computing service offering known as Infrastructure as a Service or (IaaS) (Armbrust et al., 2010). This study doesn't seek to identify security risks of the Platform as a Service (PaaS) or Software as a Service (SaaS) cloud computing services, nor does it recommend mitigation strategies for any of the identified security risks (Armbrust et al., 2010).

Time frame. The literature review collects materials only with recent copyright dates. Leedy and Ormrod (2001) recommend selecting recently written books because it is "more likely to give you a sense of current perspectives in your field and alert you to recent research finding that may be pertinent to your research problem" (p. 65). Accordingly the resources chosen for the study have copyright dates after January 1, 2001.

Selection criteria. Literature used in the study is retrieved from Google Scholar, WorldCat, the ACM Digital Library, IEEE Computer Society Digital Library, IEEE Xplore, in addition to professional and scholarly articles located with the University of Oregon article indexes located at http://onesearch.uoregon.edu. Leedy and Ormrod (2001) outline minimum standards for evaluating the acceptability of materials considered in the literature review. In accordance with Leedy and Ormrod (2001), preference is given to authors who are affiliated with an accredited university and are peer reviewed. In addition, preferred material has a stated research question or problem and a logical organization. Furthermore, the author presents

previous research and provides a set of procedures that can be replicated. Finally, the author presents a logical and valid conclusion.

Data Analysis Plan Preview

Materials that are selected for data analysis are analyzed through the use of content analysis. Leedy and Ormrod (2001) define content analysis as a detailed examination of the set of materials for the purpose of identifying patterns or themes. The first step in the analysis is defining the research problem or question (Leedy & Ormrod, 2001).

The study uses conceptual analysis to support the coding process, which is a type of content analysis (Busch et al., 2005). “In conceptual analysis, a concept is chosen for examination, and the analysis involves quantifying and tallying its presence” (Busch et al., 2005 para. 1).

Writing Plan Preview

The writing plan describes the approach taken to the presentation of the findings of the data analysis process. This study structures the findings thematically to identify similarities that allow new connections or cross-currents to be formed between unrelated research to identify important concepts (Gray & Malins, 2004).

The goal is to present themes that emerge during data analysis in relation to the two central concepts that support the purpose of the study; first, what are the C.I.A. security objectives as these are defined in the C.I.A. security model, and second how that model maps to the identified security risks in the IaaS cloud computing structure.

Definitions

The definitions section of the paper provides a framework for readers to better understand this study. The terms defined in this section are related to the C.I.A. Triad, the IaaS mode of cloud computing services, or both. Definitions are presented to reduce ambiguity and provide background for readers unfamiliar with cloud computing terminology.

Amazon Web Services (AWS) - A selection of cloud computing services offered over the Internet by Amazon.com (Mather et al., 2009).

Application Programming Interface (API) - APIs serve as building blocks for programmers putting together software applications. In the context of cloud computing, APIs are interfaces for programmers to accessing and manipulating cloud resources (Mather et al., 2009).

Application Virtualization - The separation of the application from the operating system. This applies to applications at all tiers, from servers to desktops. Normally, this is achieved using encapsulation. Encapsulating and isolating the application from the operating system changes the way applications can install and interact with the operating system. This makes it possible for the application to be moved from one system to another, patched, and updated without interactions with other applications or operating systems. Application virtualization also allows applications to be copied or backed up as a single file (Velte, Velte, & Elsenpeter, 2010, p. 315).

Application Service Provider (ASP) - a business that provides computer-based services to customers over a network (Mather et al., 2009, p. 293).

Asymmetric Encryption – A two key system used for data encryption. The public key is used for encryption and the private key is used for decryption of data (Mather et al., 2009).

Authentication – Determining the identity of an individual or computer system (Mather et al., 2009).

Attack Surface – An attack surface includes all the points of entry through which an adversary can gain access to a system and potentially cause damage (Manadhata, 2010).

Authorization – Granting access rights to resources or functions (Mather et al., 2009).

Availability – The assurance that the data is accessible when it is needed by authorized users (Greene, 2006)

Capsules – An application that has been had its operating system emulated in order to allow it to run on different host operating systems. This emulation frees the application to run on different operating systems without the application being aware of any changes in its environment. "With encapsulation, the application's operating system dependency has been broken" (Velte et al., 2010, p. 315).

C.I.A. Triad - The Triad stands for Confidentiality, Integrity and Availability. An attack against either or several of the elements of the C.I.A. triad is an attack against the Information Security of the organization. Protecting the C.I.A. triad means protecting the assets of the company (Greene, 2006)

Cloud Computing Incidents Database (CCID) – This is an organization that records and monitors verifiable, noteworthy incidents that affect cloud computing providers. These incidents include outages, security issues, and breaches. The organization records incidents as they happen and on an historical basis (Mather et al., 2009).

Cloud Service Provider (CSP) - A cloud service provider is a vendor of cloud computing services available over the Internet (Mather et al., 2009).

Cloud App – A software program this is not run from on-premises computer hardware, but is run on remote systems via Internet (Velte et al., 2010).

Cloud Arcs – Stands for architectures, which are software applications designs that are intended to be accessed from remote systems over the Internet (Velte et al., 2010).

Cloud Bridge – The practice of creating an application so that different components are integrated within multiple cloud environments. An example could be bridging an application between one ore more private, public or hybrid clouds (Velte et al., 2010).

Cloud Client - A computing device for cloud computing. This could be as simples as an Internet connected personal computer (Velte et al., 2010).

Cloud Lock-In – The ability of the cloud computing services subscriber to migrate an application and data from one cloud provider to another location. The ability to migrate data and applications from a cloud computing provider back to your organization. Variables determining Cloud Lock-In include time, level of difficulty, and portability (Velte et al., 2010).

Cloud OS – Another way to describe Platform as a Service (PaaS) offerings like Google App Engine or, Salesforce.com. The Cloud OS is a development environment for applications, not merely an operating system on which to run programs (Velte et al., 2010)

Cloud Portability - The ability of the cloud computing services subscriber to migrate an application and data from one cloud provider to another location. The ability to migrate

data and applications from a cloud computing provider back to your organization (Velte et al., 2010).

Cloud Provider - A provider that makes data processing services such as storage, software, or an operating system available to others over a network (Velte et al., 2010).

Cloud Service Architecture (CSA) - An architecture in which applications act as services on the Internet. The process of building services in the cloud for other developers, with the understanding that important consumers of these services could also be residents of the same cloud (Barr, 2008; Velte et al., 2010).

Cloud Storage - Storing data on a cloud provider's storage remote infrastructure. This is data storage that does not reside in local, on-premises systems. An example of this service is Amazon Simple Storage Service (Amazon S3). This service stores data off-site with access over the Internet (Velte et al., 2010).

Cloudburst - A euphemism used when an organization's cloud services are not available or have been breached by hackers or other intruders (Velte et al., 2010).

Cloudcenter - A large service provider like Google, or Amazon Web Services that rents its infrastructure. A datacenter where cloud computing services are housed (Velte et al., 2010).

Cloud-Oriented Architecture (COA) – A software development architecture that is intended to support incorporating cloud computing components (Velte et al., 2010)

Cloudsourcing – Making use of cloud computing services of any kind for an organization (Velte et al., 2010).

Cloudware – Software that is intended to create, deploy, and maintain applications in a cloud computing environment. Examples of cloudware include hypervisor software from VMWare or Xen (Velte et al., 2010).

Confidentiality - Not all data owned by the company should be made available to the public. Failing to protect data confidentiality can be disastrous for an organization (Greene, 2006)

Denial of Service or Distributed Denial Of Service (DoS), (DDoS) - A type of network-based attack that attempts to make computer or network resources unavailable to their intended users. An extremely large request for services causes the resource to appear unavailable (Mather et al., 2009, p. 294).

Elastic Compute Cloud (EC2) - An Amazon Web Services commercial web service that allows customers to rent computers on which to run their own computer applications. Amazon offers customers rental of different virtual machines (Mather et al., 2009, p. 294).

Encapsulation - Defining an application and all of its dependencies, and then locating them in a physical, isolated folder (Velte et al., 2010, p. 317).

External Cloud - A cloud computing environment that is external to the organization. The physical infrastructure does not reside in on-premises datacenters. On-premises datacenters are private clouds, which are hosted on an organization's internal infrastructure (Velte et al., 2010).

Hardware Virtualization - Software that emulates hardware to allow multiple operating systems, multiple instances of a single operating system, or any combination thereof to run on the same physical machine. The operating system is not ware that it is not actually

running on real hardware. VMware hypervisor software is an example of this type virtualization (Velte et al., 2010).

Hybrid cloud - An environment consisting of internal or external providers where an organization may run non-core applications in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud (Velte et al., 2010, p. 317).

Hypervisor - Software that controls the layer between the hardware operating systems. It allows multiple operating systems to run on the same physical hardware. There are two types of hypervisors: Bare metal, which allows the hypervisor to run directly on the hardware and hosted architecture, in which the hypervisor runs on top of an existing operating system (Velte et al., 2010, p. 317).

Integrity - Data integrity means protecting data from being tampered with by an unauthorized source (Greene, 2006)

Internal Cloud – This is another name for a private cloud. This type of cloud computing services exists within the on-premises systems an organization. These services a run on local machines and are not accessed over the Internet (Velte et al., 2010).

National Institute of Standards and Technology (NlST) - A standards organization and measurement standards laboratory and is a non-regulatory agency of the U.S. Department of Commerce (Mather et al., 2009, p. 295).

Network Virtualization - Mapping two disparate networks into a single, unified network. This makes it appear as if all remote networks are in a single place (Velte et al., 2010, p. 317).

OS Virtualization - The creation of a separate run-time environment within the same operating system. Applications are installed and interaction with the operating system is not

changed, so there are no substantial changes occurring to the host operating system (Velte et al., 2010, p. 317).

Paravirtualization - A virtual server technique that emulates hardware for a guest operating system. Paravirtualized servers are modified guest operating systems existing on top of the hypervisor The chief difference between a virtual machine and a paravirtualized machine is that the guest operating system on a virtual machine is unmodified, while the operating system in a paravirtualized environment is modified to work more directly with the hypervisor (Velte et al., 2010, p. 317).

Physical-to-Physical Migration (P2P) - Moving a complete operating system environment and installed applications from one physical server to another. This is done either by cloning drives and putting the cloned drive into a new server, or by using application virtualization to control the transfer from server to server (Velte et al., 2010, p. 318).

Physical-to-Virtual migration (P2V) - The process of capturing and migrating a complete operating system environment and applications from a physical to a virtual environment. (Velte et al., 2010, p. 318)

Private cloud - An offering that emulates public cloud computing, but on a private network housed in an organizations on-premises datacenters (Velte et al., 2010).

Public cloud - A cloud service that is provided by a third-party vendor from one or multiple data centers, and offered to multiple customers over the Internet. This is unlike a private cloud which relies on an organization's internal equipment (Mather et al., 2009).

Secure Shell (SSH) - Enables secure communications over a computer network using a network protocol that allows data to be exchanged between two networked devices using data encryption (Mather et al., 2009).

Server Virtualization – Software that enables the ability to host multiple operating systems on a single hardware platform. The supervisor or hypervisor software emulates the hardware for each operating system. The operating systems are not aware that they are not running on actual computer hardware (Velte et al., 2010).

Service-Level Agreement (SLA) - Is a part of a service contract where the level of service is formally defined. An example could be formalizing the amount of data throughput a digital circuit must pass in a give time period (Mather et al., 2009).

SPI - An acronym that represents the three major services provided in public cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The SPI acronym is a commonly used term for describing these three cloud computing service delivery models (Mather et al., 2009).

Storage Virtualization - The abstraction of physical storage from logical storage. Storage may consist of storage pools and devices in different physical locations, but the process of storage and retrieval is transparent to the end user who would only see it as a centrally managed repository (Velte et al., 2010).

Symmetric Encryption – The encryption of data, using a single secret key for both the encryption and decryption processes, unlike public key encryption (Mather et al., 2009).

SysTrust - An auditing framework that is developed by the AICPA and Canadian Institute of Chartered Accountants (CICA) to provide a mechanism for service providers to complete an audit based on a predefined set of criteria that is consistent with the C.I.A. Triad model. The SysTrust framework defines standards for availability, processing integrity, security and maintainability (Mather et al., 2009; McPhie, 2000).

Thin Client – "A client machine that performs very little data or application processing – the processing is done in the server, and the client machine processes the output for the screen display" (Dewire, 1998, p. 347)

Utility Computing - A metered computer service in which applications and or storage is available on a needed basis, very similar to the way that domestic consumers purchase utilities such as water, gas, and so on for their homes. The customers pay for only the portion of the services that they actually consume (Velte et al., 2010).

Virtual Appliance - A minimalist virtual machine image designed to run a virtualization technology (like VMware). Virtual appliances aim to eliminate the installation, configuration, and maintenance costs associated with running complicated software. The difference between a virtual machine and a virtual appliance is that a virtual appliance is fully preinstalled and preconfigured, while a virtual machine is ready for software to be installed (Velte et al., 2010, p. 318).

Virtualization - The creation of a virtual environment that supports the creation and maintenance of virtual operating systems, storage devices, applications, or network resources (Mather et al., 2009).

Virtual Machine (VM) - A server emulating real hardware for an unmodified guest operating system. The virtual machine runs as a normal software program would on the host operating system which runs on the physical hardware. Applications installed on the virtual machine are not aware that they exist on a virtual machine (Velte et al., 2010).

Virtual Private Cloud (VPC) – Analogous to a virtual private network (VPN), but the cloud version of it. It is one way to bridge private clouds to a public cloud (Velte et al., 2010).

Virtual-to-Physical migration (V2P) - The method of installing a virtual operating system, applications and data onto a physical server (Velte et al., 2010).

Research Parameters

This study is designed as a literature review. A "literature review provides the meaningful context of your project within the universe of already existing research" (Obenzinger, 2005, p. 1). A good review of the literature "evaluates, organizes, and synthesizes what others have done" (Leedy & Ormrod, 2001, p. 77). The research parameters presented below include a central research question and sub questions. In addition, the documentation approach is described in detail including the processes used to store, classify and code the resources found for the literature review.

Research Questions

Crafting a novel research question requires that it must be placed in the context of current and previous research to qualify it as worthy of recognition in the field (Obenzinger, 2005). The main issue is how the security of the IaaS model of cloud computing is measured using the C.I.A. model.

1. What is the C.I.A. model and what categories of security does it address?
2. What security risks are identified when using the IaaS model of cloud computing?
    a. What points in the cloud computing system are vulnerable to attack
    b. What subsystems are vulnerable to attack
    c. What layers of the system are vulnerable to attack, for example; network, application, or physical?
3. How do the identified security risks map to the C.I.A. security model?

Search Report

The literature search focuses on finding and locating literature that is written on the subjects of cloud computing technologies, and computer security concepts and practice. Some of the literature on computer security concepts and practice may not specifically address the security problems of cloud computing, but is used to provide context to frame the problem for the audience

Data collection process. Creswell (2009) recommends building a set of search terms (key words) to use in locating literature in an academic library. “These key words may emerge in identifying a topic or may result from preliminary readings” (Creswell, 2009, p. 29). Creating the list of search terms is an iterative process of performing searches in various database portals and recording the results for refinement. Data collection is accomplished by using the search terms to find materials through the University of Oregon library portal.

Search terms. Search terms are gathered from articles, books, conference papers, and websites published on the subjects of computer security and cloud computing. The key search terms used are:

- cloud computing
- computer security
- data security
- security model

In addition to the raw results, the ACM Digital Library output provides a list of 100 discovered search terms. The researcher edits these terms further in order to create a more refined list of search terms. The researcher further refines and combines this list of search terms

in an iterative manner with the original terms to create a working set of search terms to use in finding literature.

- infrastructure
- platform
- attack
- policies
- security
- encryption
- virtual machine
- access control
- security policies
- data management
- segmentation

Types of literature sought. There are a variety of different types of literature included in the study that are germane to the subject of cloud computing and computer security. Creswell (2009) recommends seeking out specific types of literature for use in this type of study; journal articles in national journals that report research studies, and then books with one or multiple authors.

Search engines. Literature used in the study is retrieved from WorldCat, the ACM Digital Library, IEEE Computer Society Digital Library, and IEEE Xplore. These are all services that the University of Oregon library system subscribes to. In addition to these paid services, Google Scholar is used to find additional information about related literature. After initial searches are completed, the ACM Digital Library and the IEEE Computer Society Digital Library stand out as the databases with the most pertinent resources for the literature search.

Search strategies. Searches are carried out first at the University of Oregon OneSearch search portal. The initial search terms are used in an iterative process. After each search is complete, a list of returned literature is recorded. In addition to displaying the found literature, the search engines display their internal search terms which aids in the process of further refining the search terms. The process of searching for literature with the key terms repeatedly refines the quality of the search terms and the resulting literature returned from the search engines. As noted above, the ACM Digital Library and the IEEE Computer Society Digital Library stand out as the databases with the most pertinent resources for this literature search.

Search Results

Searches using the Academic Search Premier database produced good results. A search using the terms cloud computing + security results in 145 hits. The ACM Guide to Computing

Literature provided many more hits with the same search terms. The IEEE Computer Society returned 100 hits, which is comparable to the Academic Search Premier database. The Google Scholar search engine returns the greatest number of results of the search engines used.

Table 1

Search Results

Search Terms	Search Engine	Results
Cloud computing + security	Academic Search Premier	145
Cloud computing + security	The ACM Guide to Computing Literature	2,391
Cloud computing + security	IEEE Computer Society	100
Cloud computing + security	scholar.google.com	28,600

The ACM Guide to Computing Literature interface provides much finer control over results filtering than the other two databases. The ACM Guide to Computing Literature allows the search to be limited to a range of years published, presentation format, publisher, author, institutions and so on. The primary advantage of using these three academic search engines in the literature search is that they index resources that are accessible to the author of the study as a student of the University of Oregon. While Google Scholar provides the largest number of search results, most of those resources are not available to the general public for free. When pertinent material is located, it is downloaded as electronic text and stored in a computer file system. Non-electronic resources are obtained via interlibrary loan from the University of Oregon interlibrary loan system. The bibliographic records of the resources are contained in an EndNote database for storage and retrieval. Currently, there are 80 items listed.

Data evaluation procedure. Data collected from the library searches is evaluated according the nine part procedure described by Leedy and Ormrod (2001).

1. Where does the article come from? In what publication?
2. What is the research question of the article
3. Does the article represent new research, or is a synthesis of older research?
4. Is the article understandable and easy to comprehend?
5. Does the article itself include a literature review?
6. Is the research repeatable?
7. Does the research methodology including data collection make sense?
8. Do you agree with the interpretation of the results of the article?
9. What is the most important part of the article that stands out to you as the reader?

Documentation Approach

Once literature is located, citations and abstracts are saved to the EndNote database file located on the author's personal computer. Abstracts are either copied or written into the EndNote database directly. Full text and scanned articles are saved first to computer hard drive, and then entered into the Personal Brain database. Here, the entire articles, citations and notes can be kept for quick search and retrieval. Personal Brain searches inside PDF files and create text indexes automatically. Along with the full text index, the APA formatted bibliographic information is attached to the actual files located internally in Personal Brain. The EndNote database contains 60 articles. The researcher has compiled 60 full text copies of the referenced articles in Adobe Portable Document Format.

Data Analysis Plan

Materials that are selected for coding as part of the larger data analysis are analyzed through the use of content analysis. Leedy and Ormrod (2001) define content analysis as a detailed examination of the set of materials for the purpose of identifying patterns or themes.

The study uses conceptual analysis to support the coding process, which is a type of content analysis (Busch et al., 2005). "In conceptual analysis, a concept is chosen for examination, and the analysis involves quantifying and tallying its presence" (Busch et al., 2005). Busch et al. (2005) describe the process as selective reduction, which is described as when "text is reduced to categories consisting of a word, set of words or phrases, on which the researcher can focus. Specific words or patterns are indicative of the research question and determine levels of analysis and generalization."

This conceptual analysis aligns with the multiple parts of the research question. The first part of the data analysis is concerned with the question, "what is the C.I.A. model and what categories of security does it address?" The second part of the data analysis is concerned with the remaining questions and sub questions. This is the part that addresses specific security questions regarding the IaaS model of cloud computing; more specifically, a) what points in the cloud computing system are vulnerable to attack, b) what subsystems are vulnerable to attack, and c) what layers of the system are vulnerable to attack, for example; network, application, or physical?

Coding of the material is an eight step process used to identify the important terms, phrases and concepts concerning the security risks of the IaaS cloud computing services, identified within the selected references (Busch et al., 2005).

1. Decide the level of analysis. At this step concepts are defined with words, groups of words and phrases. The core concept of C.I.A. security is defined by such words as confidentiality, integrity, availability. The core concept of cloud computing includes coding terms such as virtual machine, infrastructure as a service, provisioning. The study is flexible in that it takes into account multiple word terms that define a single concept.

2. Decide how many concepts to code for. The study codes for two primary concepts; C.I.A. security objectives, and IaaS cloud services. Other concepts may emerge during the coding which may necessitate adding more corresponding coding terms.

3. Decide whether to code for existence or frequency of a concept. The study codes only for the existence of a concept, not the frequency at which it occurs. For example, the term virtual machine is coded only once per reference, even if it appears many times. However, variations in meaning of the term are coded separately.

4. Decide on how to distinguish among concepts. Concepts with comparable meanings are coded in the same categories. For example, virtual machine and virtual computer are coded under the same concept.

5. Develop rules for coding your texts. Rules are developed so that more specific terms are categorized into more generalized supersets of terms. For example, rules exist that ensure that the term *physical layer security* is part of the superset of terms labeled *network security.*

6. Decide what to do with irrelevant information. Irrelevant terms are ignored.

7. Code the texts. Text coding is handled with manual notation. Any spreadsheet program such as Microsoft Excel or Open Office is used to tabulate the coding results for each source of material. The data is stored in the Excel format or in comma separated value format.

Additionally, open source computerized analysis tools such as “Gate” (http://gate.ac.uk/) are used to accelerate the capture into a spreadsheet program.

8. Analyze your results. After the selected references are coded, conclusions are presented according to the Writing Plan section of the study.

Writing Plan

The writing plan describes the approach taken to the presentation of the findings of the data analysis process. Rapple (2010) puts forth several organizational patterns for structuring the literature review including differing theoretical approaches, concepts or methodologies. In addition to these methods, a thematic approach may yield results better than organizing the study chronologically or by author (Rapple, 2010). This study structures the findings thematically to identify similarities that allow new connections or cross-currents to be formed between unrelated research to identify important concepts (Gray & Malins, 2004; Literature reviews, 2007).

The results of the data analysis are described in detail to describe linkages between the following three themes: (a) a definition and description of the C.I.A. security model; (b) the potential security risks when using the IaaS model of cloud computing; and (c) alignment of the identified security risks in the IaaS model to the C.I.A. model.

Annotated Bibliography

The literature review is based on information derived from a set of key selected references, which are listed in this Annotated Bibliography. The materials listed are reviewed for relevance in relation to the two main concepts that are part of the purpose; how the C.I.A. model of security objectives is applied to the identified security risks in the Infrastructure as a Serviced mode of cloud computing service offerings. Bell and Smith (2009) outline guidelines for acceptability of materials considered in the literature review. Bell and Smith (2009) list these questions as a starting point for evaluating the credibility of a resource:

- Who is the author?
- What are the author's credentials?
- What is the author's reputation among his/her peers?
- Who is the publisher?
- Is the author associated with a reputable institution or organization?

In accordance, preference is given to authors who are affiliated with an accredited university and are peer reviewed. In addition, the author either creates or edits the abstract and comments sections discussing the credibility and relevance of the work to the concepts of the Literature Review.

Antonopoulos, N., Gillam, L., & SpringerLink. (2010). Cloud computing principles, systems and applications, from http://dx.doi.org/10.1007/978-1-84996-241-4

Abstract. With the growing adoption of cloud computing as a viable business proposition to reduce both infrastructure and operational costs, an essential requirement is to provide guidance on how to manage information security risks in the cloud. In this

chapter, security risks to cloud computing are discussed, including privacy, trust, control, data ownership, data location, audits and reviews, business continuity and disaster recovery, legal, regulatory and compliance, security policy and emerging security threats and attacks. Finally, a cloud computing framework and information asset classification model are proposed to assist cloud users when choosing cloud delivery services and deployment models on the basis of cost, security and capability requirements.

Comments. This reference describes the security risks of cloud computing when examined under the C.I.A. framework. The primary editor of this work, Dr. Nikolaos Antonopoulos is head of the Head of School of Computing and Mathematics, Assistant Dean (Research) of Faculty of Business, Computing and Law at the University of Derby Derby Derbyshire U.K. The editor is a respected expert in the field and this reference is judged credible for this study. This reference is selected for coding as part of the data analysis portion of the study.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D. , Rabkin, A., Stoica, I., Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58. doi: 10.1145/1721654.1721672

Abstract. The authors of this eBook acknowledge the intense interest in cloud computing from both academic and commercial organizations. They discuss the evolution of virtualized computing services and attempt to frame them in the context of earlier technologies such as software as a service and platform as a service. In addition, they examine the different economic models for various service offerings from commercialized services and open source solutions. Still another subject that the authors touch on is the topic of data integrity and security, as many potential customers may be

wary of housing their sensitive data in systems outside of their physical control. The authors also discuss the technology behind the service offerings which relies on the virtualization of software and or entire computing platforms. The work attempts to cut through the hype surround the technology and services to describe the service offerings and the potential risks in utilizing these systems. In the section labeled "Cloud Breaks" there is a discussion of security.

Comments. The article's section on Data Confidentiality/Auditability is directly related to the study's topic. This article is considered a good resource because it appears in a peer-reviewed journal. This reference is selected for coding as part of the data analysis portion of the study.

Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing. Retrieved from http://www.cloudsecurityalliance.org/csaguide.pdf

Abstract. This electronic article serves as a guideline for managing security for cloud computing services. The first section covers cloud computing technical aspects and architecture. The second section covers governances and risk management. The third section covers cloud computing operating procedures.

Comments. Rich Mogull is the founder of Securosis, L.L.C., an independent security consulting firm. He has over 17 years experience in information security, physical security, and risk management. He is one of the world's premier authorities on data security technologies and has covered issues ranging from vulnerabilities and threats, to risk management frameworks, to major application security. Glenn Brunette is the Senior Director for Enterprise Security Solutions at Oracle where he leads a team with expertise in information security, governance, risk management and compliance. Glenn is a

founding member of the Cloud Security Alliance and an OpenSolaris Security Community Leader. Glenn is a frequent author, contributor and speaker on a variety of information security and cloud computing security topics. Glenn is a Certified Information Systems Security Professional (CISSP) and has a Master's Degree in Computer Science from St. Joseph's University. This article included in the study because it contains information about virtual machines, which are a component of the IaaS architecture.

Canal, V. (2005). On information security paradigms Retrieved December 3, 2010, from https://www.issa.org/Library/Journals/2005/September/Aceituno%20Canal%20-%20On%20Information%20Security%20Paradigms.pdf

Abstract. This article discusses the various computer security models available including the C.I.A. triad and its derivatives. The author argues that security can't be purchased like a product would, but is more like a process. He goes on to point out that security costs money and is dependent upon context.

Comments. The author is experienced in a range of computer technologies and works for the BBC, Mellon Bank, and IBM. This article is written for the Information Systems Security Association, which is a special interest group specializing in global information security. This article frames the C.I.A. Triad in terms of other methodologies and concepts used to describe security as a process.

Dawoud, W., Takouna, I., & Meinel, C. (2010, 28-30 March 2010). *Infrastructure as a service security: challenges and solutions.* Paper presented at the 7th International Conference on Informatics and Systems (INFOS).

Abstract. Cloud Computing represents a new computing model that poses many demanding security issues at all levels, e.g., network, host, application, and data levels. The variety of the delivery models presents different security challenges depending on the model and consumers' Quality of Service (QoS) requirements. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer affects the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. This paper presents an elaborated study of IaaS components' security and determines vulnerabilities and countermeasures. Finally, as a result of this research, we propose a Security Model for IaaS (SMI) to guide security assessment and enhancement in IaaS layer.

Comments. The reference is an academic paper that frames the security risks of the IaaS model within the framework of the C.I.A. model. The primary author is a researcher in computer science at the University of Potsdam in the Hasso Plattner Institute for Software Systems Engineering Potsdam, Germany. This reference is selected for coding as part of the data analysis portion of the study.

Friedman, A. A., & West, D. M. (2010). Privacy and security in cloud computing. Issues in technology innovation (Brookings Institution), no.3. Retrieved from http://www.brookings.edu/papers/2010/1026_cloud_computing_friedman_west.aspx.

Abstract. This document explores how to think about privacy and security on the cloud. It is not intended to be a catalog of cloud threats. We frame the set of concerns for the cloud and highlight what is new and what is not. We analyze a set of policy issues that represent systematic concerns deserving the attention of policy-makers. We argue that the

weak link in security generally is the human factor and surrounding institutions and incentives matter more than the platform itself. As long as we learn the lessons of past breakdowns, cloud computing has the potential to generate innovation without sacrificing privacy and security.

Comments. The reference is an academic paper that frames the security risks of cloud computing within the C.I.A. and other models from a high level. The primary author is a Ph.D. researcher in computer science at the Brookings Institution in Washington DC and is a fellow in Governance Studies and research director of the Center for Technology Innovation. His current research focuses on information technology policy, with particular emphasis on cyber security policy and the dynamics of information privacy.

Furht, B., & Escalante, A. (2010). Handbook of cloud computing. New York: Springer.

Abstract. Handbook of Cloud Computing includes contributions from world experts in the field of cloud computing from academia, research laboratories and private industry. This book presents the systems, tools, and services of the leading providers of cloud computing; including Google, Yahoo, Amazon, IBM, and Microsoft. The basic concepts of cloud computing and cloud computing applications are also introduced. Current and future technologies applied in cloud computing are also discussed. Case studies, examples, and exercises are provided throughout.

Comments. This book covers most of the technical aspects of cloud computing. This book speaks directly about the cloud computing architecture including the IaaS model and general security concerns of that model. The editor, Borko Furht, Ph.D., is Chairman & Professor of the Department of Computer Science & Engineering at Florida Atlantic University. His Ph.D. is in Electrical and Computer Engineering at the University of

Belgrade, Yugoslavia, 1978. He is considered a good source of information on cloud computing security, therefore this resource is considered credible.

Gilliam, D. P. (2004). Managing information technology security risk. *Software Security - Theories and Systems, 3233*, 296-317. doi: 10.1007/978-3-540-37621-7_16

Abstract. Information Technology (IT) Security Risk Management is a critical task for the organization to protect against the loss of confidentiality, integrity, and availability of IT resources and data. Due to system complexity and sophistication of attacks, it is increasingly difficult to manage IT security risk. This paper describes a two-pronged approach for managing IT security risk: 1) an institutional approach, that addresses automating the process of providing and maintaining security for IT systems and the data they contain; and 2) a project life cycle approach that addresses providing semi-automated means for integrating security into the project life cycle. It also describes the use of a security template with a risk reduction/mitigation tool, the Defect Detection and Prevention (DDP) tool developed at the Jet Propulsion Laboratory (JPL).

Comments. This reference is important to the study because it lays the foundations of the C.I.A. security model. This reference is considered credible because the author is an IT Security Engineer at the Jet Propulsion Laboratory and is a credible author on the subject of Information Technology Security. This reference is selected for coding as part of the data analysis portion of the study.

Hayes, B. (2008). Cloud computing. *Communications of the ACM, 51*(7), 9-11.

Abstract. This article presents a high level view of cloud computing. It presents a non-technical introduction and is useful to the study as background to the study.

Comments. This article serves to introduce the history and current state of cloud

computing. This reference is considered credible for the study because it appears in a peer reviewed journal, and it has been cited in 28 other works.

Ibrahim, A. S., Hamlyn-Harris, J., & Grundy, J. (2010). *Emerging security challenges of cloud virtual infrastructure.* Paper presented at the Asia Pacific Software Engineering Conference 2010 Cloud Workshop, Sydney, Australia.

Abstract. The cloud computing model is rapidly transforming the IT landscape. Cloud computing is a new computing paradigm that delivers computing resources as a set of reliable and scalable intern net-based services allowing customers to remotely run and manage these services. Infrastructure-as-a-service (IaaS) is one of the popular cloud computing services. IaaS allows customers to increase their computing resources on the fly without investing in new hardware. IaaS adapts virtualization to enable on-demand access to a pool of virtual computing resources. Although there are great benefits to be gained from cloud computing, cloud computing also enables new categories of threats to be introduced. These threats are a result of the cloud virtual infrastructure complexity created by the adoption of the virtualization technology.

Breaching the security of any component in the cloud virtual infrastructure significantly impacts on the security of other components and consequently affects the overall system security. This paper explores the security problem of the cloud platform virtual infrastructure identifying the existing security threats and the complexities of this virtual infrastructure. The paper also discusses the existing security approaches to secure the cloud virtual infrastructure and their drawbacks. Finally, we propose and explore some key research challenges of implementing new virtualization aware security solutions that can provide the preemptive protection for complex and ever dynamic cloud virtual

infrastructure. This reference is selected for coding as part of the data analysis portion of the study.

Comments. This paper provides background information that specifically describes the security problems related to the IaaS model of cloud computing. The primary author is a Ph.D. Candidate and a member of the Faculty of Information & Communication Technologies at Swinburne University of Technology in Australia. The paper directly illustrates the threats to VMs, and the hypervisor software that runs them they are used in the IaaS services model.

Jensen, M., Gruschka, N., Schwenk, J., & Iacono, L. L. (2009). On technical security issues in cloud computing. *2009 IEEE International Conference on Cloud Computing, 0*, 109-116. doi: http://doi.ieeecomputersociety.org/10.1109/CLOUD.2009.60

Abstract. The Cloud Computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure (CapEx) and operational expenditure (OpEx). In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security and trust issues, since the user's data has to be released to the Cloud and thus leaves the protection-sphere of the data owner. Most of the discussions on these topics are mainly driven by arguments related to organizational means. This paper focuses on technical security issues arising from the usage of Cloud services and especially by the underlying technologies used to build these cross-domain Internet-connected collaborations.

Comments. This paper describes the actual modes of security attacks on all three of the cloud computing services offers, including (IAAS). The paper is subsequently published

in the IEEE Explore Database. This source is a reputable professional organization. This reference is selected for coding as part of the data analysis portion of the study.

Julisch, K., & Hall, M. (2010). Security and control in the cloud. *Information Security Journal: A Global Perspective, 19*(6), 299-309.

Abstract. Cloud computing is a new IT delivery paradigm that offers computing resources as on-demand services over the Internet. Like all forms of outsourcing, cloud computing raises serious concerns about the security of the data assets that are outsourced to providers of cloud services. To address these security concerns, we show how today's generation of information security management systems (ISMSs), as specified in the ISO/IEC 27001:2005, must be extended to address the transfer of security controls into cloud environments. The resulting virtual ISMS is a standards-compliant management approach for developing a sound control environment while supporting the various modalities of cloud computing. This article addresses chief security and/or information officers of cloud client and cloud provider organizations. Cloud clients benefit from our exposition of how to manage risk when corporate assets are outsourced to cloud providers. Providers of cloud services learn what processes and controls they can offer in order to provide superior security that differentiates their offerings in the market.

Comments. The article contains background on the security management of all three modes of cloud computing services; IaaS, PaaS, and SaaS. Klaus Julisch has a Ph.D. in Computer Science from the University of Dortmund, Germany, and more than 10 years of experience in information security. Michael Hall is the Practice Development Partner at Forbes Sinclair, an international risk management advisory company with offices in Madrid, Spain, and Tampa, Florida. This article is useful in creating context in which to

view the research question. This source is published in a reputable, peer reviewed journal and this source is judged credible.

Jinzhu, K. (2010). *A practical approach to improve the data privacy of virtual machines*. Paper presented at the 2010 10th IEEE International Conference on Computer and Information Technology. Bradford, UK.

Abstract. Cloud computing can provide users dynamically scalable, shared resources over the Internet, but users usually fear about security threats and loss of control of data and systems. This paper presents a practical architecture to protect the data confidentiality for guest virtual machines. With this solution, even the cloud computing service providers cannot access the private data of their clients. This is very important and attractive for the cloud clients. In our work, we utilize virtualization technology and trusted computing technology to construct a secure and robust virtualization platform. On this platform, we customize the guest virtual machine operating system, strengthen the isolation between virtual machines, and therefore, greatly improve the data privacy of cloud services. With our solution, the cloud service provider can compromise the availability, but not the confidentiality of the guest virtual machines.

Comments. This paper discusses a central concept of the IaaS infrastructure model; the use of virtual machines to provide computing services to consumers. It discusses in detail the methods used to ensure the privacy of a virtual machine and the applications and data contained in it. This source is published in a reputable, peer reviewed journal and this source is judged credible. This reference is selected for coding as part of the data analysis portion of the study.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE, 7*(4), 61-64. doi: http://doi.ieeecomputersociety.org/10.1109/MSP.2009.87

Abstract. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. In this new world of computing, users are universally required to accept the underlying premise of trust. Within the cloud computing world, the virtual environment lets users access computing power that exceeds that contained within their own physical worlds. Typically, users know neither the exact location of their data nor the other sources of the data collectively stored with theirs. The data you can find in a cloud ranges from public source, which has minimal security concerns, to private data containing highly sensitive information (such as social security numbers, medical records, or shipping manifests for hazardous material). Does using a cloud environment alleviate the business entities of their responsibility to ensure that proper security measures are in place for both their data and applications, or do they share joint responsibility with service providers? The answers to this and other questions lie within the realm of yet-to-be-written law. As with most technological advances, regulators are typically in a "catch-up" mode to identify policy, governance, and law. Cloud computing presents an extension of problems heretofore experienced with the Internet. To ensure that such decisions are informed and appropriate for the cloud computing environment, the industry itself should establish coherent and effective policy and governance to identify and implement proper security methods.

Comments. This reference is useful to the study because it introduces the C.I.A. security objective in a non-technical manner. This reference appears in a reputable professional journal, the IEEE Xplore Digital Library, and has been cited in three other articles.

Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I. (2010). Cloud migration: a case study of migrating an enterprise it system to IaaS.

Abstract. This case study illustrates the potential benefits and risks associated with the migration of an IT system in the oil & gas industry from an in-house data center to Amazon EC2 from a broad variety of stakeholder perspectives across the enterprise, thus transcending the typical, yet narrow, financial and technical analysis offered by providers. Our results show that the system infrastructure in the case study would have cost 37% less over 5 years on EC2, and using cloud computing could have potentially eliminated 21% of the support calls for this system. These findings seem significant enough to call for a migration of the system to the cloud but our stakeholder impact analysis revealed that there are significant risks associated with this. Whilst the benefits of using the cloud are attractive, we argue that it is important that enterprise decision-makers consider the overall organizational implications of the changes brought about with cloud computing to avoid implementing local optimizations at the cost of organization-wide performance.

Comments. The reference is germane to the study because it discusses an actual case study of an organization migrating on-premises system to an IaaS service offering of Amazon.com. The paper is subsequently published in the ACM Digital Library. This source is a reputable professional organization.

Khajeh-Hosseini, A., Sommerville, I., & Sriram, I. (2010). Research challenges for enterprise

cloud computing.

Abstract. Cloud computing represents a shift away from computing as a product that is purchased, to computing as a service that is delivered to consumers over the Internet from large-scale data centers – or 'clouds'. This paper discusses some of the research challenges for cloud computing from an enterprise or organizational perspective, and puts them in context by reviewing the existing body of literature in cloud computing. Various research challenges relating to the following topics are discussed: the organizational changes brought about by cloud computing; the economic and organizational implications of its utility billing model; the security, legal and privacy issues that cloud computing raises. It is important to highlight these research challenges because cloud computing is not simply about a technological improvement of data centers but a fundamental change in how IT is provisioned and used. This type of research has the potential to influence wider adoption of cloud computing in enterprise, and in the consumer market too.

Comments. This is an academic paper submitted to the Submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010. The reference is germane to the study because it discusses the nature of attacks on existing cloud computing infrastructure. The paper is subsequently published in the ACM Digital Library. This source is a reputable professional organization. This reference is selected for coding as part of the data analysis portion of the study.

Krutz, R. L., & Vines, R. D. (2010). *Cloud security: a comprehensive guide to secure cloud computing*. Indianapolis, IN: Wiley.

Abstract. Cloud computing allows for both large and small organizations to have the

opportunity to use Internet-based services so that they can reduce start-up costs, lower capital expenditures, use services on a pay-as-you-use basis, access applications only as needed, and quickly reduce or increase capacities. However, these benefits are accompanied by a myriad of security issues, and this book tackles the most common security challenges that cloud computing faces. The authors offer expertise and knowledge as they discuss the extremely challenging topics of data ownership, privacy protections, data mobility, quality of service and service levels, bandwidth costs, data protection, and support.

Comments. This reference examines both the C.I.A. triad security model and the IaaS mode of cloud computing services in detail. The primary author is considered knowledgeable in the field of computer security and cloud computing. The primary author is a Ph.D. in electrical engineering and is currently a visiting lecturer at the Computer Forensics Program of the University of New Haven (Nemeh, 2008). The author writes publications on microprocessors and logic design; develops video tape courses on microprocessors and software; contributes articles to professional journals. In addition the author is awarded seven patents for computer and digital systems.

This reference is selected for coding as part of the data analysis portion of the study.

Marks, E. A., & Lozano, B. (2010). Executive's guide to cloud computing. Hoboken, N.J.: Wiley.

Abstract. This book is a non-technical guide to cloud computing for business leaders. The book promotes the power of cloud computing to dominate the marketplace, using the low cost, highly capable technologies of cloud computing.

Comments. This reference is useful in framing cloud computing in the larger context of on-premises dedicated data processing operations. Eric A. Marks is President and CEO of AgilePath Corporation, a Service-Oriented Architecture (SOA) and Web services solutions firm, with seventeen years of experience in the field, and lectures at Syracuse University's nationally recognized School of Information Studies. Roberto (Bob) Lozano is chief strategist and founder of Appistry, Inc., a leading provider of cloud application platforms and lectures on artificial intelligence as an adjunct faculty member at Washington University in St. Louis.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy. Beijing; Cambridge [Mass.]: O'Reilly.

Abstract. This book reviews the current state of data security and storage in the cloud, including confidentiality, integrity, and availability. In addition, there is discussion of the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services. This work also discusses which security management frameworks and standards are relevant for cloud computing

Comments. This volume covers topics such as network and physical layer security in relation to the IaaS, Saas, and PaaS services. Specifically the book examines virtual server security, which is an important aspect of the IaaS model. In addition, all three authors are respected experts in the field of computer security. This volume is judged to be credible on the basis of the amount of industry and government experience the authors possess in information security management.

Mell, P., & Grance, T. (2010). The NIST definition of cloud computing. [Article]. *Communications of the ACM, 53*(6), 50-50.

Abstract. The authors set out to create definitions for the technology behind cloud computing service offerings. For example, they make distinctions between Software as a Service and Platform as a Service. They break the terminology down into three sections including “Essential Characteristics,” “Service Models,” and “Deployment Models.”

Comments. This source is published in a reputable, peer reviewed journal. It provides valuable background and sets the IaaS model in context to the other cloud computing models such as PaaS, and SaaS.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds*. Paper presented at the Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA.

Abstract. Third-party cloud computing represents the promise of outsourcing as applied to computation. Services, such as Microsoft’s Azure and Amazon’s EC2, allow users to instantiate virtual machines (VMs) on demand and thus purchase precisely the capacity they require when they require it. In turn, the use of virtualization allows third-party cloud providers to maximize the utilization of their sunk capital costs by multiplexing many customer VMs across a shared physical infrastructure. However, in this paper, we show that this approach can also introduce new vulnerabilities. Using the Amazon EC2 service as a case study, we show that it is possible to map the internal cloud infrastructure, identify where a particular target VM is likely to reside, and then instantiate new VMs until one is placed co-resident with the target. We explore how such

placement can then be used to mount cross-VM side-channel attacks to extract information from a target VM on the same machine.

Comments. This paper documents an actual attack method used against the Amazon EC2 environment, which is an example of an IaaS service offering. The authors describe the security pitfall of placing VMs on the same physical server, which makes them vulnerable to hacker attacks which can take control of the machines. This reference is an academic paper written by a Ph.D. candidate at University of California, San Diego. The Author is now a member of the faculty of the Department of Computer Sciences at the University of Wisconsin, Madison. This reference illustrates one of the modes that C.I.A. security can be compromised when using IaaS service offerings. This reference is selected for coding as part of the data analysis portion of the study.

Rittinghouse, J. W., & Ransome, J. F. (2010). Cloud computing: implementation, management, and security. Boca Raton: CRC Press.

Abstract. Presenting an understanding of what cloud computing really means, this title explores how disruptive it may become in the future, and examines its advantages and disadvantages. It gives business executives the knowledge necessary to make informed, educated decisions regarding cloud initiatives.

Comments. This book contains information on server virtualization, which is an integral portion of the IaaS cloud computing model. John W. Rittinghouse is Chief Software Architect and Co-founder of Hypersecurity LLC in Houston, Texas. He holds a Ph.D. in Psychology with emphasis in Natural Language Processing. James F. Ransome is a Senior Director and the Chief Security Officer for the Cisco Collaborative Software

Group (WebEx). He holds a Ph.D. in Information Systems specializing in Information Security.

Sangroya, A., Kumar, S., Dhok, J., Varma, V., & Conference. (2010). Towards analyzing data security risks in cloud computing environments.

Abstract. There is a growing trend of using cloud environments for ever growing storage and data processing needs. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. This paper primarily aims to highlight the major security issues existing in current cloud computing environments. We carry out a survey to investigate the security mechanisms that are enforced by major cloud service providers. We also propose a risk analysis approach that can be used by a prospective cloud service for analyzing the data security risks before putting his confidential data into a cloud computing environment.

Comments. This reference is an academic paper describing the security implications of cloud computing. In addition the researchers survey the field of cloud computing vendors to determine the level of security mechanisms available for the range of services available. The primary researcher is a graduate student employed as a research assistant for the Software Engineering Research lab (SERL), Department of Computer Science, IIIT Hyderabad, India. This reference is selected for coding as part of the data analysis portion of the study.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems recommendations of the National Institute of Standards and Technology, from http://purl.access.gpo.gov/GPO/LPS23533

Abstract. This is a technical guide from the National Institute of Standards and technology that describes good security practices for information systems management.

Comments. This reference lays the groundwork for examining risk management for computerized information systems. The author is an electrical engineer creating guidelines for the National Institute of Standards and Technology, a government agency. In addition the author is technical advisor to the Federal Information Security Management Act implementation project. Stoneburner is the author or co-author of many special publications in the NIST SP 800 series on information security, and he is considered to be an expert in the field of computer security.

Stoneburner, G. (2001). Underlying technical models for information technology security. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

Abstract. The purpose of this document is to provide a description of the technical foundations, termed 'models', that underlie secure information technology (IT). The intent is to provide, in a concise form, the models that should be considered in the design and development of technical security capabilities. These models encompass lessons learned, good practices, and specific technical considerations.

Comments. This reference lays the groundwork for defining models used in describing computer security. The author is an electrical engineer creating guidelines for the National Institute of Standards and Technology, a government agency. In addition the author is technical advisor to the Federal Information Security Management Act implementation project. Stoneburner is the author or co-author of many special publications in the NIST SP 800 series on information security, and he is considered to be an expert in the field of computer security.

Subashini, S., & Kavitha, V. (2011). Review: A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11. doi: 10.1016/j.jnca.2010.07.006

Abstract. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model. A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. The architecture of cloud poses such a threat to the security of the existing technologies when deployed in a cloud environment. Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment. In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.

Comments. This reference describes the security problems inherent in the IaaS deliver model of cloud computing. The author describes how the IaaS delivery model does away completely with the need for physical data centers, but only provides only basic security systems such as firewalls and load balancing. This reference is a article appearing in an academic journal by post graduate student and his advisor at the Anna University Tirunelveli, India. It is considered a credible reference for this study. This reference is selected for coding as part of the data analysis portion of the study.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review, 39*(1), 50-55. doi: 10.1145/1496091.1496100

Abstract. This paper discusses the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20 definitions have been studied allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches.

Comments. This reference lays the foundation for a definition of cloud computing. The authors surveyed multiple definitions of cloud computing in order to survey the field and look for common themes and concepts. The primary author, is a Ph.D. researcher with Hewlett-Packard Labs, an information technology and services company. This reference is considered a credible reference for this study. This reference is selected for coding as part of the data analysis portion of the study.

Velte, A. T., Velte, T. J., & Elsenpeter, R. C. (2010). *Cloud computing : a practical approach*. New York: McGraw-Hill.

Abstract. This book addresses the costs, benefits, security issues, regulatory concerns, and limitations related to cloud computing systems. Commercial offerings such as Google, Microsoft, Amazon, Yahoo, IBM, EMC/VMware, Salesforce.com, and others are described

Comments. This book contains an overview of cloud computing technologies. It is useful to the study because it provides context for cloud computing services. Anthony T. Velte, CISSP, CISA, is an award-winning author and cofounder of Velte Publishing, Inc. Toby J. Velte, Ph.D., is an international, bestselling, award-winning author of business technology articles and books. Robert Elsenpeter is an award-winning author and journalist. This resource is published by a major publisher, McGraw-Hill, and is written by three editors who are considered experts in the field, one of which is a doctor of philosophy.

Wang, C., Ren, K., Lou, W., & Li, J. (2010). Toward publicly auditable secure cloud data storage services. *IEEE Network, 24*(4), 19-24.

Abstract. Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-

level requirements. In order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on-demand data correctness verification on behalf of cloud data owners have to be designed. In this article we propose that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public auditability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed. Such an auditing service not only helps save data owners¿ computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. We describe approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality.

Comments. This article is concerned with creating a framework to quantify the security of data stored on the cloud. This is germane to the study, because this is how data is stored in the IaaS model; in virtual machines within a cloud service provider. Cong Wang is currently a Ph.D. student in the Electrical and Computer Engineering Department at Illinois. Kui Ren is an assistant professor in the Electrical and Computer Engineering Department at Illinois Institute of Technology. He obtained his Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute in 2007. Wenjing Lou, Ph.D. is an assistant professor for the University of Florida. She joined the Electrical and Computer Engineering She is a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) award in 2008. Jin Li, PhD is an associate senior researcher in the Electrical and Computer Engineering Department at Illinois Institute of

Technology. The authors of this article are considered experts in the field. This resource appears in a peer reviewed journal.

Wei, J., Zhang, X., Ammons, G., Bala, V., & Ning, P. (2009). *Managing security of virtual machine images in a cloud environment*. Paper presented at the Proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA.

Abstract. Cloud computing is revolutionizing how information technology resources and services are used and managed but the revolution comes with new security problems. Among these is the problem of securely managing the virtual-machine images that encapsulate each application of the cloud. These images must have high integrity because the initial state of every virtual machine in the cloud is determined by some image. However, as some of the benefits of the cloud depend on users employing images built by third parties, users must also be able to share images safely. This paper explains the new risks that face administrators and users (both image publishers and image retrievers) of a cloud's image repository. To address those risks, we propose an image management system that controls access to images, tracks the provenance of images, and provides users and administrators with efficient image filters and scanners that detect and repair security violations. Filters and scanners achieve efficiency by exploiting redundancy among images; an early implementation of the system shows that this approach scales better than a naive approach that treats each image independently.

Comments. This reference describes the risks involve in the use of VMs in the IaaS mode of cloud computing. The reference is an academic paper describing a proposed security system which scans VM images for security violations or flaws. The primary author received his Ph.D. in Computer Science from the Georgia Institute of Technology

in 2009. This reference is selected for coding as part of the data analysis portion of the study.

Westby, J. R., & Allen, J. H. (2007). Governing for enterprise security implementation guide, from http://www.cert.org/archive/pdf/07tn020.pdf

Abstract. Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security is not be articulated, achieved, or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.

This implementation guide builds upon prior publications by providing prescriptive guidance for creating and sustaining an enterprise security governance program. It is geared for senior leaders, including those who serve on boards of directors or the equivalent. Throughout the implementation guide, we describe the elements of an enterprise security program (ESP) and suggest how leaders can oversee, direct, and control it, and thereby exercise appropriate governance. Elevating security to a governance-level concern fosters attentive, security-conscious leaders who are better positioned to protect an organization's digital assets, operations, market position, and reputation. This document presents a roadmap and practical guidance that helps business leaders implement an effective security governance program.

Comments. This article provides context for the subject of computer security. There is no mention of cloud computing Ms. Westby serves as Adjunct Distinguished Fellow to

Carnegie Mellon CyLab, the largest university-based cyber security research and education institute in the United States. She is a member of the bars of the District of Columbia, Colorado and Pennsylvania and the American Bar Association. Ms. Westby is the author of numerous articles on information security and speaks globally on privacy, security, cybercrime, outsourcing, Homeland Security, and legal issues pertaining to the use of technology. Julia Allen is a senior Member of Technical Staff of the Carnegie Mellon Software Engineering Institute. She is the author of The CERT Guide to System and Network Security Practices (Addison-Wesley, June 2001), Governing for Enterprise Security (CMU/SEI-2005-TN-023, 2005), the CERT Podcast Series: Security for Business Leaders, and co-author of Software Security Engineering: A Guide for Project Managers (Addison-Wesley, May 2008).

Whitman, M. E., & Mattord, H. J. (2004). Management of information security. Boston, Mass.; United Kingdom: Thomson Course Technology.

Abstract. Management of Information Security primarily focuses on the managerial aspects of information security, such as access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. The third edition includes up-to-date information on changes in the field such as revised sections on national and international laws and international standards like the ISO 27000 series. With these updates, Management of Information Security continues to offer a unique overview of information security from a management perspective while maintaining a finger on the pulse of industry changes and academic relevance.

Comments. This book discusses information security from a non cloud computing viewpoint. It is valuable to the study because this work discusses specific types of attacks on network resources. Dr. Whitman is a PhD in Management Information Systems from Auburn University, Alabama. Dr. Whitman is the Director of the KSU Center for Information Security Education, since he founded the Center in 2002.

Review of the Literature

The review of the literature for this study identifies the security risks of the Infrastructure as a Service delivery mode using the C.I.A. security model as a template.

Description of the C.I.A. Security Model

The C.I.A. security model is a way of describing the information security level of a system; the model dates back to mainframe computing (Whitman & Mattord, 2004). The term *C.I.A. Security Model* is synonymous with the terms *C.I.A. Triad* and *C.I.A. Triangle* (Brunette & Mogull, 2009; Greene, 2006; Whitman & Mattord, 2004). The C.I.A. acronym stands for "confidentiality," "integrity," and "availability" (Gilliam, 2004). Data stored electronically in computers are valuable assets and should be protected against unauthorized disclosure, unauthorized tampering or destruction and obstructions to availability; attacks against one or more of these items are considered an attack on an organization's information security (Greene, 2006).

Confidentiality refers to the ability to control the access to information that should remain secret to those individuals or groups who are not authorized to view that information (Pfleeger & Pfleeger, 2007; Whitman & Mattord, 2004). In addition, only those individuals who have a demonstrated need may access such materials (Whitman & Mattord, 2004). Confidentiality of information is also defined as secrecy or privacy (Pfleeger & Pfleeger, 2007). Ensuring confidentiality or the secrecy of sensitive materials such as intellectual property or medical records is a critical issue (Gilliam, 2004). Many enterprises consider their intellectual property more valuable than physical assets, so establishing and maintaining policies and mechanisms that guard intellectual property is a critical part of maintaining competiveness in the market (Liu &

Kuhn, 2010). The failure to ensure the confidentiality of data stored within an electronic system results in an organization experiencing a damaged reputation, embarrassment or even possible legal ramifications (Stoneburner et al., 2002).

In cloud computing systems confidentiality is related to the areas of "... intellectual property rights, covert channels, traffic analysis, encryption, and inference" (Krutz & Vines, 2010, p. 63). Intellectual property is protected by *copyright laws* which protect inventions, designs, art, music and literary works (Krutz & Vines, 2010). A *covert channel* is an unauthorized and unintended communications session that allows the exchange of information (Krutz & Vines, 2010). *Traffic analysis* is the process of examining the volume, source and destinations of network traffic to make inferences about what types of information is being transmitted (Krutz & Vines, 2010). *Encryption* is the scrambling of messages into code to guard against eavesdropping (Krutz & Vines, 2010). *Inference* is the ability for individuals to gain information about data stored out of reach at a higher security level by analyzing the data that they do have access to (Krutz & Vines, 2010).

Integrity of information requires that three conditions are met: (a) unauthorized persons or systems can not modify data; (b) authorized persons or systems can not make unauthorized changes to data; and (c) the data is internally and externally consistent, that is the internal structures within the data are consistent and the relation of this data to the real world is consistent (Krutz & Vines, 2010). In addition, integrity refers to the quality of stored information that ensures that it is not corrupt, and exists in whole (Whitman & Mattord, 2004). Loss of data integrity can result from malicious or accidental damage, corruption, destruction, alteration or other tampering (Gilliam, 2004; Whitman & Mattord, 2004). If the loss of data integrity is not

corrected, then the continued use of the compromised data can lead to faulty business decisions, other inaccuracies, or even fraud (Stoneburner et al., 2002)

Availability refers to the ability of an authorized user or system to access data and information processing services without difficulty (Whitman & Mattord, 2004). Since availability entails access to data and data processing services, it is harder to define than confidentiality and integrity (Pfleeger & Pfleeger, 2007). A system is available if: (a) there is a timely response to a request, (b) all requestors are treated equally, (c) the service employs fault tolerance to minimize downtime due to hardware failure, and (d) the system is easily accessed and appropriate mechanisms are in place to handle simultaneous access, deadlocks, and exclusive access (Pfleeger & Pfleeger, 2007). In the realm of cloud computing, CSPs define availability merely as the ability to connect to their services over the network (Habib, Ries, & Muhlhauser, 2010).

Availability is analogous to the library patron who expects access to the correct materials after providing the required identification or authorization (Whitman & Mattord, 2004). Any degradation of data availability can quickly affect an organization's efficiency and operational effectiveness when end users are expected to be productive (Stoneburner et al., 2002). An example of the loss of availability is illustrated by the case of an employee changing the name of an important file in a credit union's computer system. Although the credit union still owned the file, it was not accessible to the computer system and this stopped all production (Bosworth, 2002). The loss of availability ranges from temporary loss of access all the way up to complete and permanent destruction of the data with no chance of repair or recovery (Bosworth, 2002).

IaaS Architecture Risks Involved When Using These Technologies

Cloud computing is defined as dynamically scalable computing resources that are available over the Internet (Jensen et al., 2009). IaaS or Infrastructure as a Service represents the lowest layer of the available cloud computing services, which also includes Software as a Service and Platform as a Service (Dawoud et al., 2010; Jensen et al., 2009). Software as a Service refers to applications provided to the client that run on the cloud computing infrastructure provided by the CSP, and is accessed by what are described as *thin clients* such as a web browser (Peng, 2009). A thin client is any machine that performs very little data processing other than creating the output for the screen display of a terminal or PC since the server is responsible for the applications and data processing (Dewire, 1998, p. 347). Desktop and business applications such as Flickr and Google Apps are examples of SaaS offerings (Dawoud et al., 2010). Platform as a Service refers to applications created by a development language that is hosted by the CSP in a cloud infrastructure (Peng, 2009). An example of a PaaS offering is an enterprise application hosted within the cloud such as Google App Engine (Dawoud et al., 2010).

Both the PaaS and SaaS layers of cloud computing resides on top of the IaaS layer:

Table 1

Overview of the three delivery modes of cloud computing

Layer	Description	Examples
Software as a Service (SaaS)	Software: commercial software access, desktop and business applications	Flickr.com Google Apps
Platform as a Service (PaaS)	Platform: information, messaging, connectivity, integration, services access	
Infrastructure as a Service (IaaS)	Infrastructure: VMs providing CPU, memory, and disk storage.	Amazon EC2 Xen

Since IaaS is the foundation layer upon which the other two delivery layers are built, (PaaS and SaaS), any security vulnerabilities in this layer affect those layers as well (Dawoud et al., 2010). At this layer, IaaS can be described as computational resources, data storage and communications (Youseff, Butrico, & Da Silva, 2008). IaaS emulates the physical apparatus that a traditional datacenter would have including the servers (the computational resources), the hard drives that store that data and all the communication equipment such as network switches (Furht & Escalante, 2010). An example of an IaaS service is Amazon's EC2 service, which offers the user a virtual server, with the CPU, memory, storage, operating system and hypervisor or system monitoring software included (Amazon elastic compute cloud; Furht & Escalante, 2010).

IaaS relies on virtual machines which are software programs that emulate hardware to increase utilization in large datacenters. Typically, three resources are available to IaaS customers; virtual machine images, servers to run those images (hypervisors), and a pool of storage to save data (Wei et al., 2009). Virtual machines and the virtual infrastructure on which they run are vulnerable to many different types of attacks including security threats between (a) the customer and the datacenter, (b) the hypervisor and the VMs, and (c) between the VMs themselves (Dawoud et al., 2010) Each of these types of attacks is examined in more detail below.

Security Threats Originating Between the Customer and the Datacenter

Virtual machine mobility. Virtual machines live their lives as disk images that are hosted on a hypervisor platform and are easily copied or transferred to other locations. This mobility is advantageous because it allows VMs to be transported to other physical machines via an image file that defines the virtual disk for that system (Dawoud et al., 2010; Garfinkel &

Rosenblum, 2005). Unfortunately, the ability to move and copy VMs poses a security risk because the entire system, applications, and data can be stolen without physically stealing the machine (Dawoud et al., 2010; Garfinkel & Rosenblum, 2005). “From a theft standpoint, VMs are easy to copy to a remote machine, or walk off with on a storage device” (Garfinkel & Rosenblum, 2005, p. 3). In addition, an offline VM machine is vulnerable to being copied over a network or to removable media, or being corrupted without having to physically stealing the hard disk (Dawoud et al., 2010). Live virtual machine migration techniques also pose potential risks because they reply on the process of copying the memory pages of the system over a network to a new machine, exposing the data and applications to eavesdropping (Dawoud et al., 2010). Finally, the ease with which VMs can be copied enables users to be more inclined to carry large amounts of potentially sensitive applications and data around on personal storage devices such as USB memory sticks, posing additional potential security risks (Garfinkel & Rosenblum, 2005).

DoS – denial of service, flooding attacks; physical and virtual network attacks. One of biggest problems for IaaS is the flooding attack. This attack consists of overloading the server hosting the IaaS services with an enormous number of requests for data processing (Jensen et al., 2009). In this scenario, the attacker sends a large amount of messages to the targeted IaaS host server in order to exhaust its memory and CPU resources resulting in the loss of availability of the server to the end users (Jensen, Gruschka, & Luttenberger, 2008). The denial of service attack is a critical problem for VMs and can indicate that the hypervisor software is allowing a single VM to consume all the system resources, starving the remaining VMs and impairing their function (Dawoud et al., 2010).

Security Threats Originating from the Host (Hypervisor)

Monitoring Virtual Machines from host. Monitoring the VM from the hypervisor software is an important part of managing and controlling the VMs (Dawoud et al., 2010). However, the system administrator, or other authorized users can abuse this capability and make changes to the operation of one or more VMs (Dawoud et al., 2010). An example of an administrative tool that could be abused in this manner is Xenaccess, which allows the administrator to access the memory of a customers' Xen VM memory while it is running, posing a security risk (Amazon EC2 is Xen based) (Dawoud et al., 2010).

Communications between virtual machines and host. All communications must pass through the hypervisor to all of the hosted VMs and at this point an attacker can inject malicious software in an attempt to eavesdrop or gain control over any or all of the systems (Dawoud et al., 2010). However, the worst case occurs when the hypervisor has been compromised by malware, since this puts all the VMs that are being hosted on that machine at risk for security breaches (Dawoud et al., 2010)

Virtual machine modification. In the IaaS model, the hypervisor represents the next lower layer of software beneath the customer's operating system, applications and data. Attacks on the hypervisor layer are attractive to hackers because of the scope of control they can gain if they can install and execute their code on this layer of the VM software (Ibrahim et al., 2010). Compromising the hypervisor means that an attacker can take control of that layer and all of the hosted virtual machines that are hosted on that machine (Ibrahim et al., 2010). An entire genre of software called VM-Based Rootkits or (VMBRs) exists (e.g. HyperJacking, BLUEPILL, Vitriol, SubVir, and DKSM). This type of software is designed to take control over the hypervisor in real

time or insert malicious software to corrupt the hypervisor software to enable control at a different time (Ibrahim et al., 2010).

Placement of malicious VM images on physical systems. The attack known as *cloud malware injection* involves creating a malicious virtual machine image and then placing that image into the hypervisor so that it is treated like a legitimate system in a collection of virtual machines (Jensen et al., 2009). If this is successful, then the malicious virtual machine image is allowed to run the adversary's code (Jensen et al., 2009).

Security Threats Originating From the VMs

Monitoring VMs from other VMs. One of the security risks encountered when using virtual machines is the lack of guaranteed isolation of the application and data when a shared resource such as memory space is utilized by multiple VMs (Youseff et al., 2008). Youseff et al., (2008) note that this performance interference problem only gets worse when systems are updated with multicore processors. Cloud servers can contain tens of VMs, and these VMs can be present in different states of operation and they are vulnerable to attack whether they are active or not (Ibrahim et al., 2010). VMs that are active are vulnerable to all of the security attacks that a conventional physical service is subject to. However, once a VM has been compromised by an attack on other VMs residing on the same physical server, they are now all vulnerable to the same attack due to the fact that each machine shares memory, disk storage, driver software and hypervisor software (Ibrahim et al., 2010).

The vulnerability that dormant VMs face is different than that faced by physical servers since they are not subject to the same attacks when their power is turned off (Ibrahim et al., 2010). This is due to the fact that even a dormant VM image is still stored as data within the

shared disk storage within a VM server and is subject to the injection of malware or other tampering attacks (Ibrahim et al., 2010).

When VMs share resources and are allowed to communicate with other VMs running on a shared hardware platform, security risks can become magnified. When two VMs are allowed to share resources, a malicious program on one or both of the VMs can violate security and privacy (Dawoud et al., 2010). "A malicious VM can potentially access other VMs through shared memory, network connections, and any other shared resources without compromising the hypervisor layer" (Dawoud et al., 2010, p. 4).

Communication between VMs. Commonly, VMs are allowed to communicate with other VMs running on the same physical equipment using channels such as the shared clipboard functions (Dawoud et al., 2010). When sharing resources such as memory, real or virtual network connections between VMs can introduce possible security risks for each machine because there is the possibility that one or more of the VMs has been compromised by malicious programs; and this can occur even if the hypervisor program has not been compromised (Dawoud et al., 2010). The VMs on which the customers run their operating systems applications and data must have high integrity because they determine the initial states of those systems, which in turn affect the security states of those machines (Wei et al., 2009). VM image integrity is an important subject because cloud computing vendors offer these image templates to unrelated customers who must rely on good image integrity to maintain a known security state (Wei et al., 2009).

In addition, some cloud vendors seek to realize further costs savings by employing third parties to build images for their customers' VMs, thus raising further questions about the initial security state of these images (Wei et al., 2009). The process of provisioning VM images with

ready made templates enables the potential for attackers to modify these images to create new unauthorized VMs or modify existing templates to propagate malware to machines that are cloned from these templates (Ibrahim et al., 2010).

Conclusions

This study provides a list of security risks reported in the selected literature that are associated with the Infrastructure as a Service (IaaS) cloud computing service offerings. Identified security risks are aligned within the C.I.A. security objectives model, in order to inform the individuals responsible for managing cloud computing systems within their organizations. Eight identified types of attacks are classified in relation to three origins and mapped to the CIA model of security risks, resulting in Table 2 below.

Table 2

Overview of IaaS security attacks mapped to the C.I.A. model

Attack Surface	Attack	Confidentiality	Integrity	Availability
Security threats originating from the host (hypervisor)	Monitoring virtual machines from host.	Security Risk	Security Risk	Security Risk
	Communications between virtual machines and host.	Security Risk	Security Risk	Security Risk
	Virtual Machine modification.	Security Risk	Security Risk	Security Risk
	Placement of malicious VM images on physical systems.	Security Risk	Security Risk	Security Risk
Security threats originating from the VMs	Monitoring VMs from other VM.	Security Risk	Security Risk	Security Risk
	Communication between VMs.	Security Risk	Security Risk	Security Risk
	Virtual machine mobility	Security Risk	Security Risk	Security Risk

Attack Surface	Attack	Confidentiality	Integrity	Availability
Security threats originating between the customer and the data center	DoS – denial of service, flooding attacks; physical and virtual network attacks	*Not Applicable*	*Not Applicable*	Security Risk

.

In almost all cases, except for DoS, the threat surfaces that IaaS presents to the CIA model result in additional security risks beyond what would be experienced in a more conventional on-premises data center. Below is a brief discussion of the eight types of attacks to which the IaaS layer is vulnerable, in relation to the risks identified in the CIA model (confidentiality, integrity, and availability).

Monitoring virtual machines from host. Confidentiality is at risk because the customers' data could be revealed affecting its secrecy from unauthorized reviewers. Integrity is at risk because the operation of the VM can be changed by unauthorized individuals which could lead to the customer's data integrity being compromised. Availability is at risk because the unauthorized hypervisor user can potentially erase, or obfuscate the customers' data.

Communications between virtual machines and host. Confidentiality is at risk because the customers' data could be intercepted by unauthorized hypervisor administrators or malware. Integrity is at risk because the operation of the VM can be changed by unauthorized hypervisor administrators or malware which could lead to loss of integrity of the customers' data. Availability is at risk because by unauthorized hypervisor administrators or malware can potentially erase, or obfuscate the customers' data.

Virtual machine modification. Confidentiality is at risk because the customers' data could be intercepted or revealed by malware injected into the VM image resulting in an untrustworthy VM. Integrity is at risk because the operation of the VM can be changed by

malware injected into the VM image which could lead to loss of integrity of the customers' data. Availability is at risk because by malware injected into the VM image can potentially erase, or obfuscate the customers' data.

Placement of malicious VM images on physical systems. Confidentiality is at risk because the customers' data could be intercepted by unauthorized, malicious VMs placed in a collection of legitimate systems. Integrity is at risk because the operation of the VM can be changed by unauthorized, malicious VMs placed in a collection of legitimate systems which could lead to loss of integrity of the customers' data. Availability is at risk because unauthorized, malicious VMs placed in a collection of legitimate systems that can potentially erase, or obfuscate the customers' data.

Monitoring VMs from other VMs. Confidentiality is at risk because the customers' data could be intercepted and or revealed by unauthorized, malicious VMs neighboring customers' legitimate VMs containing their data and applications. Integrity is at risk because the operation of the VM can be changed by unauthorized, malicious VMs neighboring customers' legitimate VMs containing their data and applications, which could lead to loss of integrity of the customers' data. Availability is at risk because unauthorized, malicious VMs neighboring customers' legitimate VMs can potentially erase, or obfuscate customer data.

Communication between VMs. Confidentiality is at risk because the customers' data could be intercepted and or revealed by utilizing VM images created by third parties containing unknown initial security states and possible malware. Integrity is at risk because the operation of the VM can be changed by utilizing VM images created by third parties containing unknown initial security states and possible malware, which could lead to loss of integrity of the customers' data. Availability is at risk because by utilizing VM images created by third parties

containing unknown initial security states and possible malware potentially erasing, or obfuscating customer data.

Virtual machine mobility. Confidentiality is at risk because the customers' data could be intercepted and or revealed during the process of VM images being migrated, copied over networks or stored in removable media. Integrity is at risk because the operation of the VM can be changed during the process of VM images being migrated, copied over networks or stored in removable media which could lead to loss of integrity of the customers' data. Availability is at risk by utilizing VM images during the process of VM images being migrated, copied over networks or stored in removable media potentially erasing, or obfuscating customer data.

DoS – denial of service, flooding attacks; physical and virtual network attacks. Availability is at risk because denial of service attacks can limit access to a VM, and in turn the customers' operating system, applications and data potentially obfuscating customer data. Confidentiality and integrity are not applicable in this case because there DoS only blocks access to the data instead of providing the attacker with methods to view or change the data.

References

Amazon elastic compute cloud. Retrieved January 24, 2011, from http://aws.amazon.com/ec2

Antonopoulos, N., Gillam, L., & SpringerLink. (2010). Cloud computing principles, systems and applications, from http://dx.doi.org/10.1007/978-1-84996-241-4

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58. doi: 10.1145/1721654.1721672

Barr, J. (2008). The emerging cloud service architecture, from http://aws.typepad.com/aws/2008/06/the-forthcoming.html

Bell, C., & Smith, T. (2009). Critical evaluation of information sources, from http://libweb.uoregon.edu/guides/findarticles/credibility.html

Bosworth, S. (2002). *Computer security handbook*. New York, NY: Wiley.

Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing. Retrieved from http://www.cloudsecurityalliance.org/csaguide.pdf

Busch, C., De Maret, P. S., Flynn, T., Kellum, R., Le, S. M., Brad, Saunders, M., . . . Palmquist, M. (2005). Content analysis. Retrieved December 12, 2010, from http://writing.colostate.edu/guides/research/content/com2b1.cfm

Canal, V. (2005). On information security paradigms Retrieved December 3, 2010, from https://www.issa.org/Library/Journals/2005/September/Aceituno%20Canal%20-%20On%20Information%20Security%20Paradigms.pdf

Chudnov, D. (2010). A view from the clouds. [Article]. *Computers in Libraries, 30*(3), 33-35.

Conry-Murray, A. (2009). What's in the public cloud: How 12 vendors are delivering on infrastructure as a service. *Information Week - Manhasset*(1240), 37-42.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, Calif.: Sage Publications.

Dawoud, W., Takouna, I., & Meinel, C. (2010, 28-30 March 2010). *Infrastructure as a service security: Challenges and solutions.* Paper presented at the 7th International Conference on Informatics and Systems (INFOS).

Dewire, D. T. (1998). Thin clients [delivering information over the web], from http://www.netlibrary.com/urlapi.asp?action=summary&v=1&bookid=1887

Friedman, A. A., & West, D. M. (2010). Privacy and security in cloud computing. *Issues in technology innovation (Brookings Institution), no.3*. Retrieved from http://www.brookings.edu/papers/2010/1026_cloud_computing_friedman_west.aspx

Furht, B., & Escalante, A. (2010). *Handbook of cloud computing*. New York: Springer.

Garfinkel, T., & Rosenblum, M. (2005). *When virtual is harder than real: Security challenges in virtual machine based computing environments*. Paper presented at the Proceedings of the 10th conference on Hot Topics in Operating Systems - Volume 10, Santa Fe, NM.

Gilliam, D. P. (2004). Managing information technology security risk. *Software Security - Theories and Systems, 3233*, 296-317. doi: 10.1007/978-3-540-37621-7_16

Gray, C., & Malins, J. (2004). *Visualizing research : A guide to the research process in art and design*. Aldershot, Hants, England ; Burlington, VT: Ashgate.

Greene, S. S. (2006). *Security policies and procedures : Principles and practices*. Upper Saddle River, N.J.: Pearson Prentice Hall.

Habib, S. M., Ries, S., & Muhlhauser, M. (2010, 26-29 Oct. 2010). *Cloud computing landscape and research challenges regarding trust and reputation.* Paper presented at the

Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC).

Hayes, B. (2008). Cloud computing: As software migrates from local pcs to distant internet servers, users and developers alike go along for the ride. *Communications - ACM, 51*(7), 9-11. doi: 10.1145/1364782.1364786

Hinchcliffe, D. (2009). What does cloud computing actually cost? An analysis of the top vendors. *Dion Hinchcliffe's Next Generation Enterprises*, from http://www.ebizq.net/blogs/enterprise/2009/08/what_does_cloud_computing_actu.php

Ibrahim, A. S., Hamlyn-Harris, J., & Grundy, J. (2010). *Emerging security challenges of cloud virtual infrastructure.* Paper presented at the Asia Pacific Software Engineering Conference 2010 Cloud Workshop, Sydney, Australia.

Jensen, M., Gruschka, N., & Luttenberger, N. (2008). *The impact of flooding attacks on network-based services*.

Jensen, M., Gruschka, N., Schwenk, J., & Iacono, L. L. (2009). On technical security issues in cloud computing. *2009 IEEE International Conference on Cloud Computing, 0*, 109-116. doi: http://doi.ieeecomputersociety.org/10.1109/CLOUD.2009.60

Jinzhu, K. (2010). *A practical approach to improve the data privacy of virtual machines*.

Julisch, K., & Hall, M. (2010). Security and control in the cloud. *Information Security Journal: A Global Perspective, 19*(6), 299-309.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE, 7*(4), 61-64. doi: http://doi.ieeecomputersociety.org/10.1109/MSP.2009.87

Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I. (2010). *Cloud migration: A case study of migrating an enterprise it system to iaas*. Paper presented at the Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing.

Khajeh-Hosseini, A., Sommerville, I., & Sriram, I. (2010). Research challenges for enterprise cloud computing. doi: http://arxiv.org/abs/1001.3257v1

Krutz, R. L., & Vines, R. D. (2010). *Cloud security : A comprehensive guide to secure cloud computing*. Indianapolis, IN: Wiley.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical research: Planning and design*. Upper Saddle River, N.J.: Merrill Prentice Hall.

Literature reviews. (2007). *The Writing Center*, from http://www.unc.edu/depts/wcweb/handouts/literature_review.html

Liu, S., & Kuhn, R. (2010). Data loss prevention. *IT Professional, 12*(2), 10-13.

Manadhata, P. K. (2010). An attack surface metric. *IEEE Transactions on Software Engineering, 99*(PrePrints).

Marks, E. A., & Lozano, B. (2010). *Executive's guide to cloud computing*. Hoboken, N.J.: Wiley.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy*. Beijing; Cambridge [Mass.]: O'Reilly.

McPhie, D. (2000). Aicpa/cica systrust principles and criteria. [Article]. *Journal of Information Systems, 14*(1), 1.

Mell, P., & Grance, T. (2010). The nist definition of cloud computing. [Article]. *Communications of the ACM, 53*(6), 50-50.

Nemeh, K. H. (2008). *American men & women of science : A biographical directory of today's leaders in physical, biological, and related sciences*. Farmington Hills, Mich.: Thomson Gale.

Obenzinger, H. (2005). What can a literature review do for me? Retrieved from http://ce.uoregon.edu/aim/Capstone07/LiteratureReviewHandout.pdf

Peng, J. (2009). *Comparison of several cloud computing platforms*.

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in computing*. Upper Saddle River [etc.]: Prentice-Hall.

Rapple, B. (2010). Writing a literature review Retrieved December 27, 2010, from http://libguides.bc.edu/litreview

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). *Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds*. Paper presented at the Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA.

Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud computing: Implementation, management, and security*. Boca Raton: CRC Press.

Sangroya, A., Kumar, S., Dhok, J., Varma, V., & Conference. (2010). Towards analyzing data security risks in cloud computing environments.

Stoneburner, G. (2001). Underlying technical models for information technology security : Recommendations of the national institute of standards and technology Retrieved from http://purl.access.gpo.gov/GPO/LPS72071

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems : Recommendations of the national institute of standards and technology Retrieved from http://purl.access.gpo.gov/GPO/LPS23533

Subashini, S., & Kavitha, V. (2011). Review: A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11. doi: 10.1016/j.jnca.2010.07.006

Talbot, D. (2010). Security in the ether. [Article]. *Technology Review, 113*(1), 36-42.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review, 39*(1), 50-55. doi: 10.1145/1496091.1496100

Velte, A. T., Velte, T. J., & Elsenpeter, R. C. (2010). *Cloud computing : A practical approach*. New York: McGraw-Hill.

Viega, J. (2009). Cloud computing and the common man. *Computer, 42*(8), 106-108. doi: 10.1109/mc.2009.252

Wang, C., Ren, K., Lou, W., & Li, J. (2010). Toward publicly auditable secure cloud data storage services. *IEEE Network, 24*(4), 19-24. doi: http://dx.doi.org/10.1109/MNET.2010.5510914

Wei, J., Zhang, X., Ammons, G., Bala, V., & Ning, P. (2009). *Managing security of virtual machine images in a cloud environment*. Paper presented at the Proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA.

Westby, J. R., & Allen, J. H. (2007). Governing for enterprise security (ges) implementation guide, from http://handle.dtic.mil/100.2/ADA472572

Whitman, M. E., & Mattord, H. J. (2004). *Management of information security*. Boston, Mass.; United Kingdom: Thomson Course Technology.

Youseff, L., Butrico, M., & Da Silva, D. (2008, 12-16 Nov. 2008). *Toward a unified ontology of cloud computing.* Paper presented at the Grid Computing Environments Workshop, 2008. GCE '08.