2016-09

Secure cloud computing implementation study for Singapore military operations

Guoquan, Lai

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURE CLOUD COMPUTING IMPLEMENTATION STUDY FOR SINGAPORE MILITARY OPERATIONS

by

Lai Guoquan

September 2016

Thesis Advisor: John D. Fulp
Co-Advisor: Gurminder Singh

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE SECURE CLOUD COMPUTING IMPLEMENTATION STUDY FOR SINGAPORE MILITARY OPERATIONS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Lai Guoquan			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Cloud computing benefits organizations in many ways. With characteristics such as resource pooling, broad network access, on-demand self-service, and rapid elasticity, an organization's overall IT management can be significantly reduced (in terms of labor, software, and hardware) and its work processes made more efficient. However, is cloud computing suitable for the Singapore Armed Forces (SAF)? How can the SAF migrate its traditional system to cloud-based services in a safe and secure manner? These were questions answered in this thesis.

In this thesis, cloud computing was shown to increase cost-effectiveness in the healthcare and business sectors. In addition, from the military perspective, the benefits of cloud computing were analyzed from a study of the U.S. Department of Defense. Then, using cloud computing–related documents from the United States, a list of recommended policy statements were developed for the SAF to consider for guidance as it migrates to greater adoption of cloud-based computing in support of its operations. These policy statements encompass the various aspects of information security deemed most important to the SAF's adoption of a cloud-based computing environment.

14. SUBJECT TERMS military cloud computing, could computing military features, military cloud computing framework			**15. NUMBER OF PAGES** 103
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SECURE CLOUD COMPUTING IMPLEMENTATION STUDY FOR SINGAPORE MILITARY OPERATIONS

Lai Guoquan
Major, Singapore Armed Forces
B.S., Nanyang Technological University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2016

Approved by: John D. Fulp
Thesis Advisor

Gurminder Singh
Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cloud computing benefits organizations in many ways. With characteristics such as resource pooling, broad network access, on-demand self-service, and rapid elasticity, an organization's overall IT management can be significantly reduced (in terms of labor, software, and hardware) and its work processes made more efficient. However, is cloud computing suitable for the Singapore Armed Forces (SAF)? How can the SAF migrate its traditional system to cloud-based services in a safe and secure manner? These were questions answered in this thesis.

In this thesis, cloud computing was shown to increase cost-effectiveness in the healthcare and business sectors. In addition, from the military perspective, the benefits of cloud computing were analyzed from a study of the U.S. Department of Defense. Then, using cloud computing–related documents from the United States, a list of recommended policy statements were developed for the SAF to consider for guidance as it migrates to greater adoption of cloud-based computing in support of its operations. These policy statements encompass the various aspects of information security deemed most important to the SAF's adoption of a cloud-based computing environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AEC	Army Experience Center
API	application program interface
C2	command and control
CNN	Cable News Network
CSA	Cloud Security Alliance
CSCC	Cloud Standards Customer Council
DISA	Defense Information Systems Agency
DOD	Department of Defense
DSTA	Defence Science & Technology Agency
FedRAMP	Federal Risk and Authorization Management Program
HADR	humanitarian assistance and disaster relief
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
IDA	Infocomm Development Authority of Singapore
IDF	Israel Defense Forces
ISP	Internet service provider
IT	information technology
MINDEF	Ministry of Defence
NIST	National Institute of Standards and Technology
PDPA	Personal Data Protection Act
PSDT	Personnel Services Delivery Transformation
RACE	Rapid Access Computing Environment
SAF	Singapore Armed Forces
SRG	security requirement guide

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The development of this thesis would not have been possible without the support of many individuals. As such, I would like to take this opportunity to extend my heartfelt gratitude to the following individuals.

First, I would like to thank my cousin, Maria Yu, who accompanied my son and me to the United States, which allowed me to pursue a master's degree program. I appreciate all she has done for us. Because of her unwavering love and care, my son was able to truly experience American culture.

Second, I would like to offer my sincere gratitude to both of my advisors, John D. Fulp and Dr. Gurminder Singh, for their patience, guidance, and commitment throughout my thesis project.

Third, I would like to thank my employer, the Singapore Armed Forces (SAF), for providing me the opportunity to further my studies in the United States.

Last, I would like to thank God, who makes all things possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS MOTIVATION

As a signal officer in the Singapore Armed Forces (SAF), I manage and maintain the SAF's defense systems, working to facilitate secure communication between different units and forces—sometimes involving foreign countries—and to ensure interoperable storage and processing of shared data. This can be difficult when the underlying infrastructure involves an amalgam of heterogeneous systems that results in having many diverse and complicated hardware and software configurations. With the increasing adoption of cloud or cloud-based computing around the globe, the SAF is interested in finding out whether cloud computing can, or should, be leveraged to improve the manageability and/or resilience of information technology (IT) systems in Singapore's military domain.

This thesis includes studies of the current implementation of cloud computing technologies and proposals for how cloud computing can be used most effectively for Singapore's military operations. The key objectives of this thesis are, first, to examine how securely and successfully cloud computing has been implemented in the commercial and private sectors and, second, to research how cloud computing can be used to support Singapore's military operations.

The result of this thesis is to explore a cost-efficient and secure enterprise—the level of security driven by the data—that can be readily adapted to Singapore's defense needs. In order to achieve the thesis objectives, the following questions were asked and answered:

- What exactly is cloud computing?
- How has cloud computing benefited commercial and private sectors in their environments?
- What security risks are inherent to cloud computing?
- Are there any cases of known cloud computing attacks that are useful as case studies for this thesis?

- What are the known best-practice security controls that are applicable to the cloud environment?
- From a networking and command-and-control (C2) perspective, how can cloud computing be used for country-level joint military operations (e.g., humanitarian assistance and disaster relief [HADR])?
- What are the cloud features necessary for cloud computing to support military operations (e.g., HADR)?

B. THESIS SCOPE AND ORGANIZATION

The research conducted as part of this thesis was organized into three main areas:

1. Research and Analysis of Existing Cloud Computing Technology

The initial area of research focused primarily on the examination of existing cloud computing technology and how it has been used over the years. This research included a detailed study of how cloud solutions have benefited the public and defense sectors. In addition, an analysis of selected case studies was conducted to identify the current threats and vulnerabilities. This information is useful as it established a baseline of typical cloud-based usage, from which it can be used to carve-out differences and/or peculiarities as might pertain to the SAF's potential deployment of same or similar cloud technology.

2. Information Security in Cloud Computing

What does it mean to say that a cloud service is secure? Does implementing tight authentication mechanisms suffice to state that the cloud is secure? This section defines information security in a cloud computing context. Research on cloud computing security threats, along with some real-life cases, was also discussed in this section.

3. Development of a Cloud Computing Framework for Singapore Military Usage

The results of this thesis included a cloud migration framework and unique military cloud features, which can be used as references when the SAF decides to adopt cloud services for its operations. This thesis covered areas such as computer security, cloud computing, and secure management of systems.

This thesis comprises seven chapters:

- Chapter I explains the motivation for conducting this research and the approach used in developing the notional the SAF cloud computing framework. In addition, the chapter presents the background and definition of cloud computing, including its advantages, challenges, and different model types.
- Chapter II presents a study of cloud computing in public sectors, such as healthcare and business, outside Singapore, highlighting various associated usage and security concerns using cloud-based services.
- With the U.S. Department of Defense (DOD) as an example, Chapter III discusses how the organization has used cloud computing to aid its military operations, developments, and advancements.
- Chapter IV focuses on Singapore's implementation of cloud computing. Results from the study of the public and defense sectors are presented.
- Chapter V discusses the objectives of information security in IT systems. In this chapter, a summary of cloud computing risks with some real-life examples are also presented.
- Chapter VI presents cloud computing recommendations and a framework for the SAF usage.
- Chapter VII provides conclusions, lessons learned, and potential research areas for this topic of study.

C. BACKGROUND

1. What is Cloud Computing?

Various organizations and authors have slightly different definitions of cloud computing. The United States Computer Emergency Readiness Team defines cloud computing as "a subscription-based service where you can obtain networked storage space and computer resources" [1]. Cisco defines cloud computing as "delivering infrastructure, services, and software on demand via the network" to cloud users [2]. International Business Machines (IBM) defines it as "the delivery of on-demand computing resources—everything from applications to data centers—over the Internet on a pay-for-use basis" [3].

Although the definitions differ slightly from one another, the fundamental concept is similar: "delivery of computing services over the Internet" [4]. In other words, consumers are able to use computing services (e.g., web hosting, email, pay-roll management, data archiving, and more) managed by third-party data centers or service providers that are likely stationed at remote locations.

Quoted from [5], National Institute of Standards and Technology (NIST) explains cloud computing with the following five characteristics:

- On-demand self-service—A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction from each service provider.

- Broad network access—Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

- Resource pooling—The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of locational independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

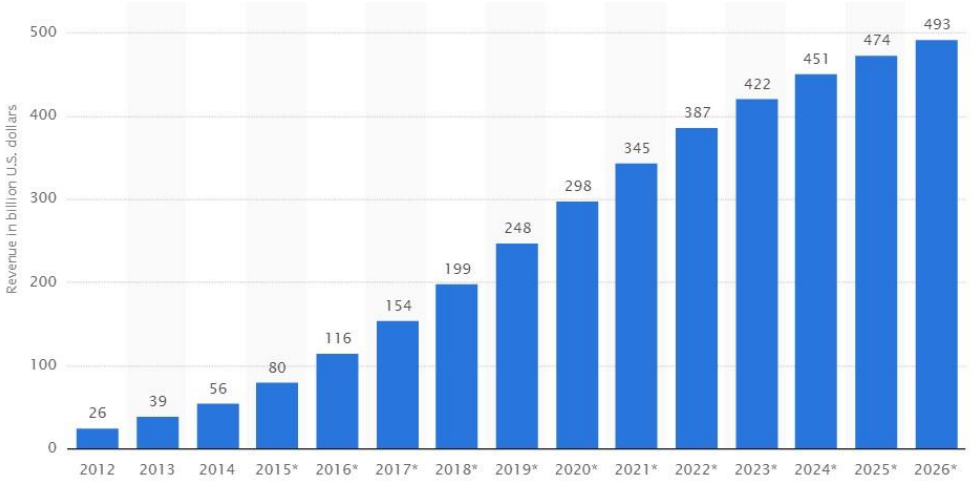
- Rapid elasticity—Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

- Measured service—Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. [5]

2. Market Trend

According to Statista [6], the public cloud computing market has shown continuous revenue growth in cloud services, beginning with a notable increase in

revenue between 2012 and 2014. This report also projects increased revenue into the next decade (see Figure 1). This implies that more and more individuals and businesses are adopting cloud-based service models. Because traditional—non-cloud—systems are more expensive (e.g., manpower and resources) and difficult to maintain, cloud computing or cloud-based sharing systems have improved by leaps and bounds, owing to marked demand for such outsourcing of IT services.



Public cloud market vendor revenue worldwide from 2012 to 2026 (in billions of U.S. dollars)

Figure 1. Revenue of the Public Cloud Market from 2012 to 2026. Source: [6]

3. Advantages of Cloud Computing

Cloud computing that utilizes a shared pool of infrastructure and resources offers many benefits. These shared resources can be in the form of data storage, power, and processing. The following describes some benefits of cloud computing [7]:

- Cost Efficiency—Since the use of a common cloud service linked by a commercial Internet service provider (ISP) is shared centrally, the shared licensing and reduced infrastructure for the software and hardware, can significantly reduce its purchase and maintenance cost.

- Almost Unlimited Storage—An individual or organization can store almost unlimited information in the cloud, assuming one has the appropriate subscription.

- Backup and Recovery—With all information stored in the cloud, performing backups and restorations is likely much more convenient than having to maintain the required resources locally.

- Improved Accessibility—Assuming connectivity infrastructure is available, cloud users can access their information stored in the cloud from virtually anywhere and at any time.

- Quick Deployment—Cloud-based services can be implemented/deployed quickly when an organization decides to subscribe to the services provided by a cloud computing provider. This can be achieved in a matter of minutes, given that the organization has Internet access to the particular provider [7].

4. Challenges of Cloud Computing

Table 1 provides a summary of the advantages and challenges of using cloud computing. Subsequent sections elaborate on the pros and cons (see Chapter II, Sections B and C).

Table 1. Advantages and Challenges of Cloud Computing. Adapted from [7].

	Advantages	Challenges
Cloud Computing	• Cost Efficiency • Almost Unlimited Storage • Backup and Recovery • Improved Accessibility • Quick Deployment	• Technical Issues • Security of the Cloud • Prone to Attack • Possible Downtime • Cost

There are many obvious benefits of cloud computing. However, as cloud computing is a shared resource, managed by a third party (i.e., a cloud provider), challenges also exist. The following are the most frequently cited challenges [7]:

- Technical Issues—Not all systems are guaranteed to run perfectly. Though it is true that cloud-hosted information can be accessed from virtually anywhere and at any time, there are circumstances when the cloud technology experiences unforeseen outages as well as other technical issues. These unexpected outages may include software and configuration errors, insufficient bandwidth, natural disasters, and cyber attacks [7].

- Security of the Cloud—Cloud providers that have direct access to the information hosted on their systems pose a serious trust-based risk to their consumers, especially when the cloud-hosted information is sensitive or

classified. In addition, anyone—including hackers—can potentially access the systems that compose a given cloud provider's infrastructure if the cloud provider has weak or otherwise ineffective security [7]. From the standpoint of security, it seems that switching to cloud computing is less than ideal. Managing Director Michael Redding of Accenture Technology Labs, which specializes in technology outsourcing, argues otherwise. He suggests that switching to the cloud can actually be beneficial, especially for small businesses. "Because large cloud computing companies have more resources, he says, they are often able to offer levels of security an average small business may not be able to afford implementing on its own servers" [8].

- Prone to Attack—Almost everyone has access to the Internet, making the information stored in the cloud prone to external hacking attacks and threats [7].

- Possible Downtime—The reliability of cloud-based services depends on both the cloud provider as well as the ISP. The services of a cloud provider can be very reliable, but if the quality of the connection from the ISP is slow or weak, cloud consumers will not realize the full potential of the cloud-based services [7].

- Cost—One assumption is that cloud computing is surely less expensive than providing the services in-house. However, this is contingent on a case-by-case cost-benefit tradeoff dependent on many factors [7].

The question, then, is how cloud computing can be implemented securely in the Singapore military context so as to reap all the potential benefits it offers without introducing excessive risk. Running a military includes the operation of many different entities. It involves complex systems to handle the administration in areas such as human resources, finance and auditing, education, counseling, defense policy and research, and logistics [9]. Can the cloud really host all these systems and services?

In after-action reports following joint military operations (e.g., exercises, disaster recovery operations, and combat operations), administrations often report the difficulties in communication among countries. Since different countries use different communication devices and systems, they have different protocols and configurations, which result in compatibility issues. In addition, with the increased number of devices connecting to the network, there can be insufficient bandwidth to fulfill the demands of all the different forces from the participating countries or units [10]. In an address during the TechNet Asia-Pacific conference in 2004, Rear Admiral (Sel.) Craig E. Bone (USCG,

Chief of Staff, 14th Coast Guard District) elaborated on the diverse challenges facing his service. He emphasized that "warfighting across half the globe requires partners that interoperate" [11]. Thus, a better, more cost-effective solution to these compatibility issues may be to incorporate cloud computing or cloud-based sharing systems among countries for resource sharing, coordination, and collaboration.

Unconventional warfare and joint operations require collaboration among countries. Military organizations may benefit from this study by using the provided framework for a top-down review of their existing cloud-service implementations. For organizations that will be incorporating cloud computing for the first time, these recommendations can be used as guidelines.

5. Cloud Computing Models

The NIST defines cloud computing as follows:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. [5]

The NIST definition of cloud computing has been used by many organizations including the Office of the Privacy Commissioner of Canada [4] and the Infocomm Development Authority of Singapore (IDA) [12]. These organizations have also adapted NIST's explanation of cloud computing services and deployment models for their work in the cloud computing environment. Contributing to a common understanding of cloud computing helps lay the foundation for implementing cloud computing solutions that are tailored to different users' needs.

a. Cloud Service Models

In "The NIST Definition of Cloud Computing," Special Publication 800–145, NIST [5] broadly divides cloud computing into three service models:

> *Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
>
> *Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
>
> *Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). [5]

From the definitions of these three service models, it may be hard to visualize how responsibilities are split between the provider and the consumer. The clear distinction of the responsibilities for each service model are shown in Figure 2, adapted from an IDA document [12].

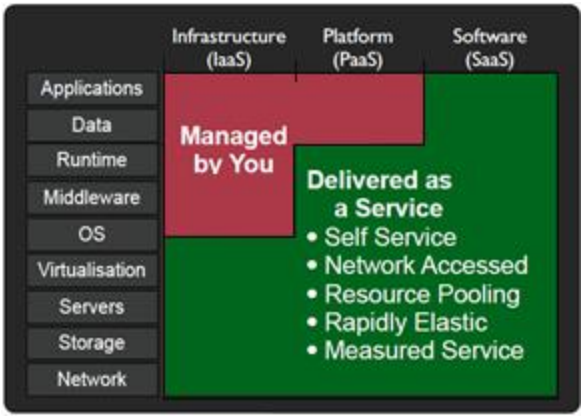


Figure 2. Division of Responsibilities by Cloud Service Models. Adapted from [12].

b. Cloud Deployment Models

Quoted from [5], NIST's Special Publication 800–145 defines the four deployment models as follows:

> *Private cloud*. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
>
> *Community cloud*. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
>
> *Public cloud*. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
>
> *Hybrid cloud*. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). [5]

D. SUMMARY

This chapter encompassed the motivation and the approach used to develop the notional the SAF cloud computing framework. A background providing an explanation of cloud computing, including its advantages, challenges, and different models, was also presented. Chapter II considers some real-world, non-Singapore cloud provider examples from the public sector.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CLOUD COMPUTING IN NON-SINGAPORE PUBLIC SECTOR

A. OVERVIEW

Many organizations in the public sector have adapted cloud computing within their operating environment to take advantage of the benefits it provides. In this chapter, we explore and examine some real-world cases with regard to healthcare and business operations.

B. CLOUD COMPUTING IN HEALTHCARE

In its report, "Impact of Cloud Computing on Healthcare," Cloud Standards Customer Council (CSCC)[1] has highlighted significant cloud computing benefits to the healthcare sector. Healthcare providers who work in different clinics and hospitals require quick access to healthcare records. Quick access to a patient's healthcare data is important because it allows healthcare providers to more quickly administer the correct treatment to the patient. In some cases, a delay in treatment can result in prolonged or added discomfort in the best case, or potential loss of life in the worst case.

The sharing of healthcare data between different locations was not possible with the traditional, non-cloud-based, IT systems. However, with the advancements in cloud computing, a cloud service (e.g., a centrally shared healthcare records database) allows healthcare providers to access and share healthcare records not only more efficiently but also more accurately. Integrating cloud technologies into healthcare operations has certainly helped improve services to the patients [13].

1. Benefits of Cloud Computing in the Healthcare Sector

Table 2 shows a summary of cloud computing benefits in the healthcare sector:

1 "CSCC is an end-user advocacy group dedicated to accelerating cloud's successful adoption, and drilling down into the standards, security and interoperability issues surrounding the transition to the cloud," quoted from About Us. (n.d.). Cloud Standards Customer Council. [Online]. Available: http://www.cloud-council.org/about-us.htm. Accessed Sep. 1, 2016.

Table 2. Benefits of Cloud Computing in Healthcare. Adapted from [13].

	Benefits
Cloud Computing	• Clinical Research • Electronic Medical Records • Collaboration Solutions • Telemedicine • Big Data • Analytics • Health Information Exchange

a. Clinical Research

In recent days, pharmacology vendors have been seen tapping the cloud to conduct research and drug development. This is primarily because vendors do not have sophisticated IT systems that have the capability of running large datasets (e.g., DNA sequencing), which is necessary for more in-depth clinical research queries. In contrast, commercial cloud vendors have developed clinical research clouds that offer this capability, not only in a less expensive way but also in a more efficient environment to carry out research.

b. Electronic Medical Records

A hospital IT department may require significant time and effort to manage an IT system that supports the sharing of electronic medical records both internally and externally (i.e., with some healthcare providers located outside of its premises). Using cloud services, managed and supported by a cloud provider (usually a third party), the hospital IT department can focus more of its resources on supporting its own in-house IT needs and less on the development and support of the larger enterprise network of cooperating healthcare providers.

c. Collaboration Solutions

The success of physician visits using remote video conferencing via the cloud has also served to promote cloud-based services elsewhere, such as rural telehealth and disaster response. With this distributed computing environment, healthcare providers on

the ground are able to communicate remotely with their headquarters for additional support.

d. Telemedicine

Cloud computing is an enabler for telemedicine. With its related processing, services, and data storage, consultations and treatments can be conducted "over the wire." Patients with smart handheld devices can connect with healthcare providers to access treatment methods such as tele-consultations, video-conferencing, and home monitoring via cloud services.

e. Big Data

A large volume of clinic data, such as radiology images and genomic data, incurs significant costs to store the information locally in traditional systems. With the advancement of technology, cloud computing has provided healthcare organizations the opportunity of storing such a high volume of data in the cloud environment with a reduced cost. In addition, with the data stored in a common location (i.e., the "cloud"), healthcare providers from different locations will be able to access it efficiently, thus minimizing delays for patient diagnosis and treatment.

f. Analysis

Analysis of healthcare-related issues, such as treatment methods, costs, and performance, requires large amounts of raw data on treatment methods, patient reactions to treatment methods, and more. Without cloud computing, it is very difficult to consolidate such large amounts of raw data for the purpose of research and analysis, especially if the data is stored separately in different healthcare providers' premises. However, if a cloud service is used, all data is stored centrally and can be easily retrieved, thus allowing for more efficient studies and research.

g. Health Information Exchange

Using the cloud, healthcare organizations will be able to exchange health information more efficiently and in a more cost-effective manner, without the need of many hardware devices [13].

2. Challenges of Using Cloud Computing in the Healthcare Sector

Although cloud computing has provided numerous benefits for the healthcare sector, as CSCC highlights, the technology also comes with its challenges [13]:

a. Security and Privacy

A patient's healthcare data can contain sensitive and private information such as names, addresses, telephone numbers, and payment information (e.g., credit card information). In some cases, healthcare providers have to abide by regulations—with regard to the handling of such sensitive data—enforced by the country in which they reside. Using the United States as an example, healthcare providers need to abide by the regulations spelled out in the Health Insurance Portability and Accountability Act (HIPAA)[2] when handling patient data. Abiding by the regulations was easier when data was stored locally in a system as opposed in the "cloud."

b. Service Reliability

A high reliability rate is expected from healthcare IT systems because patients' lives can be at stake, especially in emergencies. However, in using the services provided by the cloud, maintaining such reliability may be difficult because it involves participation from more than a single entity.

The reliability of cloud-based services depends not only on the cloud provider but also on the ISP—and in some cases other cloud providers. A cloud service provider delivers the cloud services, but the ISP provides the connection to these services.

[2] "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information, " quoted from a Summary of the HIPAA Security Rule. (n.d.). Department of Health and Human Services. [Online]. Available: http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/. Accessed Sep. 1, 2016.

Furthermore, some cloud service providers work with other providers to meet high performance rates. This working relationship affects the reliability of a cloud service in that it depends on all cloud providers involved, not only on the subscribed cloud provider.

c. Integration and Interoperability

Participants (e.g., surgeons, pediatricians, nurses, and billing staffs) from the healthcare sector have different terminologies and requirements when performing their tasks. For example, a billing staff requires a patient's address information, but this information is unnecessary for a surgeon. Thus, it is important to design an end-to-end cloud service that fully integrates all patient information (e.g., treatments, medications, and billing), which requires standardization. In addition, the subscribed cloud services must be interoperable with existing healthcare systems that are not suitable for the cloud environment.

d. Data Portability

Another reason why healthcare organizations are reluctant to use cloud services is their data portability. Healthcare organizations that choose to use cloud services have to ensure healthcare data can be transferred to and back from the subscribed cloud provider without any difficulties. For example, in the event that a cloud provider decides to terminate its services or refuse access to the data, a healthcare organization loses its capability to perform its tasks. Therefore, termination rights should be clearly spelled out in contractual agreements, allowing the transfer of data back to the healthcare organization or another cloud service provider if applicable [13].

C. CLOUD COMPUTING IN BUSINESS

Running a business using cloud-based services can reap many benefits. The business and industry portal of Queensland Government highlights that these services not only provide business owners an easily set-up "virtual office" but also allow them to connect to their virtual offices from almost anywhere. To access the cloud's data, business owners require only a web-enabled browser with connectivity to the Internet, which is available to most modern smart devices (e.g., tablets and smartphones). The

following sub-sections explain the benefits of a business operating in the cloud environment instead of using a traditional system [14].

1. Benefits of Cloud Computing in the Business Sector

In Table 3, a summary of the cloud computing benefits of the business sector is provided. In addition, a more detailed explanation of the pros and cons is given in subsequent sections.

Table 3. Benefits of Cloud Computing for the Businesses Sector. Adapted from [14].

	Benefits
Cloud Computing	• Reduced IT Costs • Scalability • Business Continuity • Collaboration Efficiency • Flexibility of Work Practices • Access to Automatic Updates

a. Reduced IT Costs

One main reason why businesses are switching to cloud computing is the reduction of overall IT costs. By using cloud-based services, business owners no longer need to purchase expensive hardware and software. Instead, they can subscribe at the cost of a subscription fee to necessary services that an appropriate cloud service provider manages and maintains. In addition, the need to hire expert IT staff to maintain a local system may be avoided by including system support and maintenance (e.g., system upgrades, services help, and support) in the contract with the cloud provider. Moreover, with less hardware operating in local premises, electrical bills may also be greatly reduced.

b. Scalability

By using cloud technology, businesses can scale their operational needs up or down quickly and efficiently to suit different situations. Businesses can rely on their

cloud service providers to handle the upgrades, avoiding the need to purchase and install expensive devices and/or software themselves. Using cloud-based services frees up a business owner's time from needing to handle IT-related issues, allowing him or her to concentrate on running the business.

c. Business Continuity

Perhaps at the "heart" of the various advantages offered by a good cloud service provider is the increased assurance that its services and hosted data are "always" available to its consumers. Thus, a business that stores its data in the cloud enjoys some peace of mind that its data is automatically backed up and protected. This effectively serves to transfer this responsibility to the cloud service provider. Whenever there is a disruption (e.g., natural disaster or power failure) to the services, the cloud service provider is expected to maintain sufficient redundancies, so it is well positioned to handle the situation, thus providing a degree of business-continuity protection for its cloud consumers. Without the use of cloud-based services, business owners need to invest additional time and resources into performing their own backups as well as other functions related to contingency planning and business continuity (e.g., writing policy, assigning roles, and conducting exercises).

d. Collaboration Efficiency

Running a business requires a lot of collaboration between different people (e.g., employees, contractors, and third parties). A cloud environment provides businesses the ability to communicate and share files from different locations, allowing the businesses to run more efficiently in terms of discussions and synchronization of data.

e. Flexibility of Work Practices

Cloud computing provides businesses the ability to allow their employees access to cloud data from almost anywhere and at any time. If an employee needs access to company data out of his or her office, the employee can connect to the "cloud office" quickly and easily.

f. Access to Automatic Updates

By subscribing to a cloud service, business owners can stipulate in the contractual agreement with the cloud provider that updates be performed automatically. This allows business owners to focus their time on running their businesses instead of worrying about running updates (e.g., software, server, and CPU updates) for their systems to run properly [14].

2. Challenges of Using Cloud Computing in the Business Sector

Table 4 summarizes the security concerns within the business sector's cloud computing technology. Skyhigh,[3] a well-known and reputable cloud service provider, revealed that many respondents (i.e., organizations) "don't know what applications and cloud services workers are using, and, worse, they don't know what information is exposed, where it is going, and with whom it is being shared" [15]. This has led to some security concerns, on which subsequent paragraphs elaborate.

Table 4. Challenges of Using Cloud Computing in Businesses. Adapted from [15].

	Security Concerns
Cloud Computing	• Loss or Theft of Intellectual Property • Compliance Violations and Regulatory Actions • Loss of Control Over End-User Actions • Contract Breaches • Diminished Customer Trust • Revenue Losses • Additional Administrations

a. Loss or Theft of Intellectual Property

Reports from Skyhigh have found that companies are increasingly storing sensitive data, including intellectual property, in the cloud environment [15]. Cyber criminals who are successful in conducting a breach into the "cloud" can gain access to

[3] As of Aug. 16, 2016, Bank of America, Comcast, Sony, Farmers, and Mitsubishi use cloud-based services provided by Skyhigh.

this sensitive data. From another point of view, certain fine print found in the services' terms and conditions—which are often not thoroughly reviewed owing to their length—disclose that the ownership of all client/user data uploaded to a cloud server transfers to the cloud service provider!

b. Compliance Violations and Regulatory Actions

Improper handling of customer data can lead to devastating circumstances for a company. This is primarily due to the data-handling regulations enforced by the company's country of origin. As a result, companies need to know exactly where their data is stored, how it is being processed, and who has the right to access it. For example, in the United States, healthcare providers need to abide by the regulations spelled out in HIPAA.[4] In Singapore, companies need to abide by the rules of the Personal Data Protection Act (PDPA)[5] whenever they collect citizens' data [16]. Under these mandates, organizations that use cloud services also need to ensure that the cloud service provider abides by the relevant regulations and rules.

c. Loss of Control Over End User Actions

It is difficult to track or prevent any employee from "stealing" information that is stored in the cloud infrastructure because the employee can connect to his own personal cloud via the Internet as well. While working in the organization and with relevant permissions given, an employee often accesses the organization's data for work purposes. However, an employee who is about to resign could make a duplicate copy of customers' details and then upload the data to his own personal cloud storage service for use when employed by another organization.

---

4 "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information," quoted from a Summary of the HIPAA Security Rule. (n.d.). Department of Health and Human Services. [Online]. Available: http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/. Accessed Sep. 1, 2016.

5 "The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use or disclose personal data for legitimate and reasonable purposes," quoted from Legislation and Guidelines. (n.d.). Personal Data Protection Commission, Singapore. [Online]. Available: https://www.pdpc.gov.sg/legislation-and-guidelines. Accessed Aug. 31, 2016.

d. Contract Breaches

Data movement in the cloud environment can lead to contractual breaches among business partners. A low-level employee (i.e., one who is positioned at the bottom of an organization's hierarchy), who typically is not be privy to the details of a business contract, may accidentally upload contractually restricted or classified information into cloud-based services, thus resulting in a violation of the contract and, in some cases, the company possibly being sued. Thus, it is important for organizations to find out exactly what services they are subscribing to and how the involved data are being handled in the "cloud." Some cloud providers have written in their contracts' fine print verbiage that indicates their right to share all uploaded data, which could potentially breach a confidentiality agreement made between the company and a business partner.

e. Diminished Customer Trust

Data breaches in the "cloud" may "inevitably result in diminished trust by customers" [15]. In December 2013, cyber criminals were able to steal U.S. retailer Target's customer data (i.e., credit and debit card numbers) which was stored in cloud-based services. The news of this breach led many of Target's customers to believe the store was no longer a safe place at which to shop [17].

f. Revenue Losses

A data breach in cloud-based services can have a negative impact on a business' revenue. For example, should customers learn about a data breach in one of their regular online shopping sites, they may no longer consider that site safe for electronic transactions involving their personal information, including credit card numbers, and shopping profile history. As a result, the customers may stop purchasing from that business, thus reducing that business' revenue [15].

g. Additional Administration

Certain regulations require organizations to send notifications to potential victims if a breach occurs in a cloud service. For example, regulations, such as HIPAA and

HITECH,[6] in the healthcare industry require these disclosures to potential victims [18]. With such regulations enforced for the cloud service, a company may incur additional "unnecessary" administrative overhead when such time could be better used running the business [15].

D. SUMMARY

This chapter explored how cloud computing can be used in the healthcare and business sectors. Examples of how cloud computing technology has aided as well as challenged the sector's operations were also provided. Using the United States as an example, Chapter III discusses how cloud computing can be best leveraged for military needs.

[6] "The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology," quoted from C. Coles. (2016, Feb. 16). 9 cloud computing security risks every company faces [Online]. Available: https://www.skyhighnetworks.com/cloud-security-blog/9-cloud-computing-security-risks-every-company-faces/. Accessed Aug. 31, 2016.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CLOUD COMPUTING IN NON-SINGAPORE DEFENSE SECTOR

A. OVERVIEW

This chapter examines how the U.S. Department of Defense (DOD) has leveraged cloud computing to aid operations in the U.S. military/defense domain. The cloud-based services identified can be used as references or starting points for the Singapore Armed Forces (SAF)'s adoption of cloud computing.

B. CLOUD COMPUTING USAGE IN THE U.S. DEPARTMENT OF DEFENSE

Senior officials from the defense sector are often skeptical about adopting the services provided by cloud computing. This sentiment is borne of the security risks, perceived or real, presented when an organization introduces a degree of dependency into its IT operations. Here, the dependency is that of relying on the cloud service provider, along with the network connection infrastructure (e.g., Internet connectivity from client premises to cloud provider premises), to store, protect, and—possibly—process mission essential data. Anyone, especially hackers and criminals with a desire to do harm, could gain unauthorized access to data stored in the cloud via the public Internet infrastructure. Notwithstanding these concerns, the DOD has made a significant move toward adopting cloud computing [19].

In 2010, the U.S. military utilized cloud computing in support of its recruitment mission. The services provided by the cloud helped identify candidate recruits with bad or questionable legal records by way of automated checks using fingerprint records [20]. Knowing the potential benefits of cloud computing, the Defense Information Systems Agency (DISA) under the U.S. Department of Defense has allocated a budget of $450 million for testing and development in the field of cloud computing [19].

1. Dynamic Marketing and Recruitment

The Army Experience Center (AEC) is an "Army pilot program designed to explore new technologies and techniques that the Army can leverage to improve the

efficiency and effectiveness of its marketing and recruiting operations" [21]. Using services provided by the cloud, the Army has been able to track recruits' participation in activities at the AEC. In addition, cloud computing integrated with social media platforms, such as Facebook, has allowed recruiters to reach out to participants more dynamically. Furthermore, Army recruiters can also access and reference potential recruits' data from any location (e.g., open-house events and recruitment centers) and at any time, thus better facilitating a more dynamic and personable recruitment process.

Two years of pilot trials showed positive recruitment results. With the newly established AEC, the Army was able to run its normal operations as before, but with a fewer number of recruiters and significant reduction in IT hardware and staff costs [21].

2. Secure Private Cloud Environment

Depending on the type of project, the cost for development and testing can be significant. Using a traditional system, DISA has experienced not only high costs in storage space but also a long procurement process to test and deploy a new project. In need of a cheaper and more efficient solution, the DISA developed a secure private cloud, known as Rapid Access Computing Environment (RACE), which can be used as a development platform. Kundra explains in [21],

> RACE, which uses virtual server technology to provide on-demand server space for development teams, aims to be more secure and stable than a traditional public cloud. RACE consists of many virtual servers inside a single physical server. By using virtualization technologies, DISA has divided the costs of provisioning and operating a single physical server among the users of the various virtual servers. This system passes cost savings on to individual teams. Within this virtual environment, users can use a self-service portal to provision computing resources in 50 GB increments with the guarantee that the environment will be secure to DOD standards. At DOD, a dedicated server environment used to take three to six weeks to provision due to lengthy procurement processes. However, RACE is able to provision functional server space to users in 24 hours. The cost for a user to obtain an environment on RACE is reasonable and can be set up with an approved Government credit card [21].

RACE can provide program developers the same level of service and availability as a traditional system. With additional security features, such as application separation

controls, components (e.g., applications, databases, and web servers) are separated from each other, minimizing damage if any one of them is compromised. Since the adoption of the RACE platform, program developers have used more than a hundred military applications for development and testing purposes [21].

3. Effective Software Development Platform

When it comes to software development, the reuse of written software code can help to significantly reduce the overall development cost of any project. A cloud-based software development environment can provide such a function, facilitating reuse of and development collaboration on software code. In addition, the cost of purchasing physical hardware can be avoided when utilizing such cloud services, thus allowing developers to test and deploy software more cost-efficiently.

According to Kundra [21], Forge.mil, a cloud-based software development platform developed by DISA for developers to reuse and collaborate on software code, has helped garner huge cost savings among various DOD organizations. DISA has highlighted that each project can save between $200 thousand to $15 million by using Forge.mil as a development platform.

Forge.mil not only helped save costs by utilizing a common licensing and support structure but also improved programing features such as version control tracking. This facilitates collaborative efforts as multiple users/programmers can work on the same software project simultaneously, with changes made by every user incorporated seamlessly into the project. Forge.mil has been tested to host many projects in an environment that provides protection for the classified software assets of the DOD [21]. Forge.mil has demonstrated that cloud computing can be used as an effective software development platform for an organization, including the military.

4. Self-Service Human Resource Solution

It was reported that employees within various human resources (HR) departments are spending a significant amount of time conducting a myriad of administrative requirements (e.g., document searches and case tracking) needed to manage personnel.

As such, introducing more customer-based self-service applications would effectively direct portions of this work to the individual customers. This is a win-win situation for both the HR staff and the customers. HR staff would enjoy reduced workload, allowing them to focus time and effort on solving more fundamental HR problems. Customers would enjoy more control and transparency regarding their data, be able to submit requests more quickly, and find answers to employment-related issues [21].

An example from the U.S. Air Force Personnel Center entails the subscription of cloud services "automating" nearly two million self-service searches per week, saving over $4 million every year. In addition, this Air Force self-service site is capable of scaling up and down to match fluctuating customer demands. Customers who had been used to waiting at least 20 minutes for search results using traditional systems now receive results in far shorter times, of about two minutes, when utilizing cloud-based technology [21].

C. SUMMARY

As described in [21], the DOD has benefited from the adoption of cloud computing. These cloud examples, which involve data that are not overly sensitive (e.g., unclassified), can be used as early adoption starting points for Singapore's military to test its IT solutions portfolio. Once some experience and lessons-learned are garnered from these early deployments or tests, Singapore may expand such cloud-based solutions to applications that are more mission-critical and/or sensitive in nature. The next chapter examines existing cloud computing implementations in Singapore.

IV. CLOUD COMPUTING IN SINGAPORE

A. OVERVIEW

Chapter I of this thesis outlined the advantages and challenges of cloud computing. Chapters II and III discussed how cloud computing can be leveraged to aid the public and defense sectors. This chapter focuses on Singapore and examines the usage of cloud computing in its industries and defense sector.

B. THE INFOCOMM DEVELOPMENT AUTHORITY'S ANALYSIS OF CURRENT CLOUD COMPUTING USAGE IN SINGAPORE

In May 2013, the Infocomm Development Authority of Singapore (IDA), the organization responsible for the development of information technology and telecommunications within Singapore, highlighted that there had been a significant shift in computing. Instead of using applications and services that reside on locally provisioned and owned operated systems, businesses and other end-user customers have been increasingly accessing these applications (e.g., word processing, storage, and computing power) through the Internet. Advancements in the field of cloud computing technology have made the use of such remotely provisioned applications and services over the Internet possible, not to mention highly competitive compared to traditional systems [22].

In order for Singapore to remain competitive in the infocomm sector, IDA has taken a strategic approach to sharpen its economic competitiveness. This involves putting emphasis on the research and development of cloud computing within Singapore. The objective is to allow more organizations and individual users to either begin or increase existing usage of cloud computing applications and services, thus enhancing Singapore's economic and warfighting efficiencies.

Figure 3 illustrates IDA's strategy in promoting cloud computing and enumerates the six "thrust" areas (see encircled red numbers 1–6).

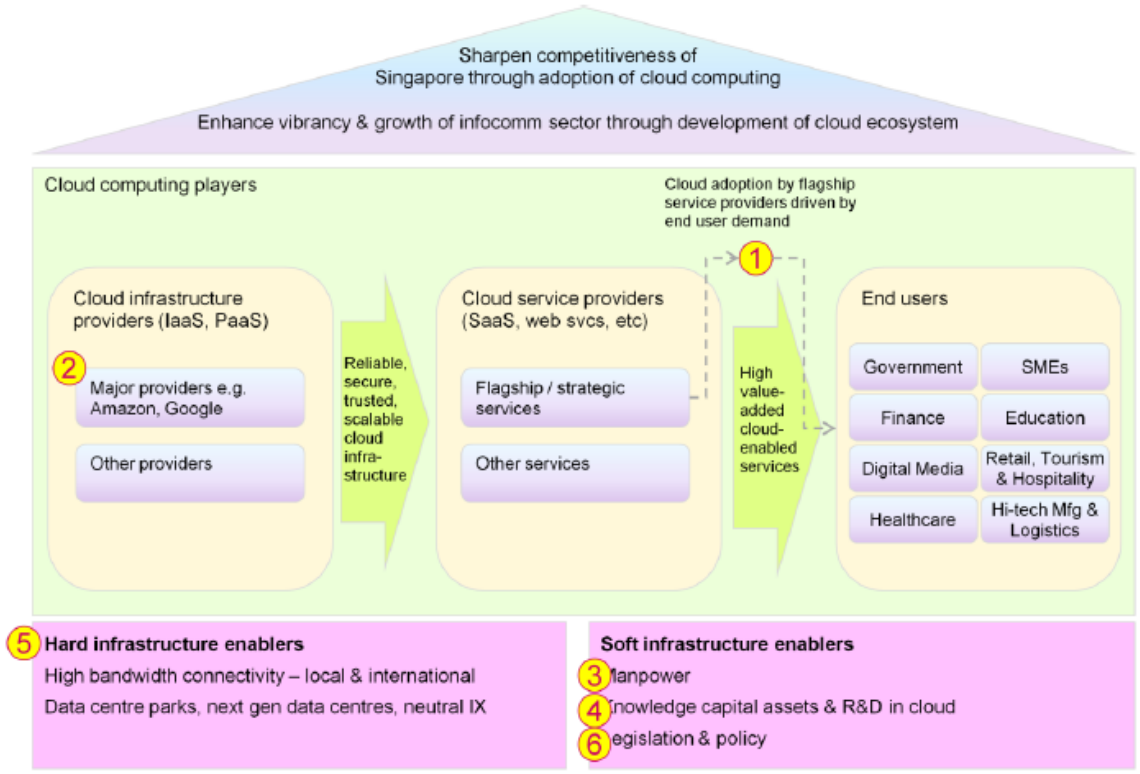


Figure 3. Six Key Thrusts. Source: [22].

Quoted from [22], the details of these six thrusts are as follows:

Thrust 1 – Support Flagship Users of Cloud Services The attraction of flagship cloud users into Singapore would lend global credibility of Singapore's capability in this space.

Thrust 2 – Attract Cloud Players Clouds require significant investment in the underlying infrastructure, such as data centres, broadband connectivity and servers, as well as in manpower resources for research and operations. Such investments are long-term and well considered business decisions.

Thrust 3 – Develop Competency for Industry & Manpower A pre-requisite to a vibrant cloud computing ecosystem is the capability of the local infocomm companies and workers exploit the new paradigm shift in order to develop innovative cloud-based services. There is a role for IDA to put in place the necessary framework and incentives for companies and workers to upgrade their competencies in this new space.

Thrust 4 – Forge R&D Relationships and Build Knowledge Capital Assets Singapore seeks to harness its existing knowledge capital resources in IHLs and RIs to attract major corporate cloud R&D to set up in Singapore.

> Investing in cloud R&D is not enough where there is a need to bridge the gap and provide a conducive environment for the translation of R&D results into industry practice and product/services deployment.
>
> Thrust 5 – Provide Enabling Infrastructure For Singapore to be a cloud computing hub to the rest of the world and region, there would be a need for world-class high speed and seamless broadband connectivity within Singapore, as well as connecting Singapore with other major cities. Development of major infocomm[7] infrastructures such as Next Gen NBN, Singapore Internet Exchange and Data Centre Park, provide a competitive environment in nurturing a vibrant cloud computing ecosystem.
>
> Thrust 6 – Build a Trusted Environment through Policy and Legislations Cloud computing investments would gravitate towards jurisdictions with stable, trusted business environment, especially when larger enterprises with mission-critical or data sensitive requirements move into the cloud. [22]

As shown in these six thrust areas, Singapore has put significant emphasis on the development of cloud computing, mainly targeted at enhancing the capability of its infocomm sector. Guided by the six thrust areas, IDA has initiated the development process of cloud computing by launching "project calls" for cloud computing proposals worth nearly $5 million. The main aim of these projects is to increase development and research in the cloud-computing domain [22].

Moreover, since November 2008, Singapore consortia led by SingTel, PTC System (S) Pte Ltd, and New Media Express Pte Ltd have offered commercial services to industry on a pay-per-use model. This model allows businesses to experiment with cloud services with minimal financial risk, as each participating business invests little in hardware, software, or infrastructure—the primary benefit of cloud computing—while having to pay only when services are actually used. These services and this pay-per-use model were also made available to government users.

Various reports have shown that government entities (e.g., statutory boards and schools) have used cloud-based services, such as video hosting and streaming, in their

[7] Infocommunications/infocomm is "the natural expansion of telecommunications with information processing and content handling functions including all types of electronic communications (fixed and mobile telephony, data communications, media communications, broadcasting, etc.) on a common digital technology base, mainly through Internet technology," quoted from Infocommunications. (n.d.). *Wikipedia*. [Online]. Available: https://en.wikipedia.org/wiki/Infocommunications. Accessed Sep. 1, 2016.

areas of work [22]. Statistics from one such report indicated that as of April 2013, 29 agencies had uploaded more than 1,000 videos using EnVision, a cloud service provider that offers hosting and streaming video services. Another report indicated that 14 schools have used EnVision's cloud services to upload videos in support of their students' activities.

In Singapore, on-going cloud computing development is evident, and there is a huge emphasis from IDA to promote the adoption of cloud computing further in government ministries and departments, statutory boards, schools, and other components of the public sector. This trend of increasing utilization of cloud services is similar to the results obtained from the research of cloud computing in public and defense sectors outside Singapore.

C. CLOUD COMPUTING IN SINGAPORE'S MINISTRY OF DEFENCE

A 2016 report from the Defence Science & Technology Agency (DSTA) titled "Private Cloud Computing"—while providing no evidence that Singapore's Ministry of Defence MINDEF has utilized any cloud computing in its operations so far—does explain the cloud infrastructure and suggest how cloud computing can provide IT services with greater agility and efficiency than traditional, in-house IT services. The report also mentions that cloud technologies, such as server virtualization and automation, have allowed new business capabilities and the optimization of data center and engineering resources [23].

As indicated by the report from DSTA [23], server virtualization and automation in cloud computing may provide the Singapore Armed Forces (SAF) with the following benefits.

1. Removal of Obsolete and Under-Utilized Systems

With cloud technology, such as server virtualization, the SAF's obsolete resources and under-utilized systems can be virtualized by shifting existing system capabilities—if still required—to cloud-based services to improve functionality. This allows IT personnel

to concentrate all upgrades and maintenance efforts on the "one-stop" virtualized cloud environment in a cost and labor effective manner.

2. Optimizing the Use of IT Resources

Most of the time, applications do not require the full computing power present in a particular system. Thus, by consolidating existing IT computing resources (e.g., central processing units and memory), the use of such resources can be optimized for different cloud-based services. In addition, the consolidated IT resources can facilitate the implementation of infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) for the SAF's cloud infrastructure.

3. Improved IT Management Process

Cloud computing can significantly improve the management of IT resources and existing systems for the SAF. With a common, shared cloud infrastructure, IT personnel can focus all upgrades and maintenance efforts at a single "cloud" location. In addition, the common cloud infrastructure eliminates the need of performing multiple updates and maintenance across different traditional systems in multiple locations.

4. Increase in Numbers of Combat Soldiers

A considerable number of conscripted national service soldiers are dedicated to the pool of IT personnel (i.e., signalers) to support and maintain existing systems for the SAF. This pool of IT personnel can be large because each military unit requires IT personnel (e.g., personnel in-charge of servers, clients, networks, and applications) to maintain the unit's system. However, if a common, shared cloud infrastructure is used, the number of IT personnel can be significantly reduced. As a result, a larger percentage of conscripted personnel can be dedicated as combat soldiers. In military jargon, this is often expressed as more teeth (fighting units) and less tail (supporting units).

5. Software Defined Infrastructure

Doctrine drives how the SAF operates. A parent unit and a sub-unit can have similar IT requirements, but to meet the requirements of the doctrine, traditional

systems—efforts of both parent and sub-unit—require considerable manual effort during the setup and configuration phases. However, with a software-defined capability in the cloud environment, IT resources and configurations for different military units can be standardized in a doctrine-driven manner.

D. SUMMARY

This chapter showed that there is emphasis being placed on cloud computing development and research in Singapore. However, the usage of cloud-based services in the SAF is not as prominent as it is in the U.S Department of Defense (DOD; see Chapter III). Thus, it may be worthwhile for the SAF—like the DOD—to leverage cloud-based services to reap the considerable benefits they provide. Since such a consideration entails a large degree of necessary "trust" regarding the competency and security of any candidate cloud service provider, Chapter V discusses information security in the context of a cloud computing environment.

V. INFORMATION SECURITY IN CLOUD COMPUTING

A. OVERVIEW

It is difficult to determine whether a system is secure without any guidance or definition. In the field of computer science, *information security* is a very board and complex term. Information security does not only cover the physical and software security aspects of a system; it also involves determining the system's reliability, trustworthiness, and resiliency to attacks. Thus, it is very important to understand the fundamental concepts and principles underlying the definition of information security. These concepts and principles are relevant in all computing environments, including the cloud. A solid foundational understanding of them allows us to employ them as guidelines regarding the proper design and implementation of the various security controls important to securing information that is stored, processed, or transmitted in and between IT systems [24]. It is for this reason that this chapter is dedicated to better understanding the essential elements of information security.

B. COMPUTER SECURITY: THE C-I-A TRIAD

Based on different views, understandings, and backgrounds, authors and researchers in the field of computer science may provide different definitions of information security. Nevertheless, the general definition of information security is actually quite brief and simple: Information security comprises all efforts (e.g., training, equipment purchasing, system configuration, certification reviews, and policy development) employed to achieve *confidentiality*, *integrity*, and *availability* of information.

Confidentiality, integrity, and availability of information, often referred to as the C-I-A triad, represent the three information-security objectives. These objectives are considered the three crucial components of security in any computer system [25]. The degree to which any given system provides these three objectives for the information that system hosts, is considered a figure of merit (i.e., a measure) for how secure that system is. Though maximum security is desired, the actual level of security achieved in any

given system environment is the outcome of a cost-benefit analysis. Such analysis seeks first to weigh the costs of providing security against the actual risk to which the system is exposed and, second, to find the correct balance among the three objectives, given the peculiar environment of the system under consideration (see Figure 4).

The aim of achieving security in information is located at the "center" of the figure where all components (equally important) of the C-I-A triad meet.

Figure 4. C-I-A Triad Model. Source: [25].

Essentially, confidentiality is a set of rules governing the access to information or data in a computer system. Integrity ensures that information is trustworthy and accurate when the information is stored or transmitted from one location to another. Availability assures timely access to information by authorized users from anywhere and at any time [25]. The following sections describe confidentiality, integrity, and availability in detail.

1. Confidentiality

Confidentiality means that only authorized personnel are permitted to access the information. The information should remain secret to those who are not authorized to access it. Unauthorized access to confidential information may result in devastating consequences. For example, terrorists who are able to access sensitive information (e.g., surveillance camera location, patrol plans, and routes) stored in a national security application may use it to their advantage. Unauthorized access can occur not only in national security applications but also in other public areas such as business industries and healthcare.

In the context of information security, the main mechanisms for protecting confidentiality are cryptography[8] and access control.[9] Some examples of threats to confidentiality are insecure networks, intruders, malware, and social engineering [25].

2. Integrity

The integrity of information involves the trustworthiness, origin, completeness, and correctness of information. Integrity, here, refers to two aspects: integrity of the information and integrity of the source of information, referred to as authenticity. Stated another way, information retains integrity only if the user of that information knows that the information has not been unintentionally or maliciously modified and the source/originator of the information (as indicated) is true and trustworthy. The basic protective mechanisms employed to achieve this security objective include hash functions and encryption [25].

3. Availability

Information availability is roughly described as assured, timely access to information. One may argue that *timely* is a rather subjective thing, and this is intended within the definition. Whether the user of some particular information in a given situation considers his or her access "timely," depends on one's circumstances at the time. For example, a person who needs emergency medical assistance requires immediate access whereas a person who is ordering a pizza can tolerate a delay. Attacks that target this information-security objective are collectively referred to as denial of service (DoS) attacks. Note that complete denial of service is not necessarily required for a DoS attack to be successful, as it may be sufficient from the attacker's perspective simply to delay access [25].

---

[8] "Cryptography is the procedures, processes, methods, etc., of making and using secret writing, as codes or ciphers," quoted from Cryptography. (n.d.). *Dictionary.com*. [Online]. Available: http://www.dictionary.com/browse/cryptography. Accessed Sep. 1, 2016.

[9] "Access control is way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information," quoted from Access Control. (n.d.). *Techopedia*. [Online]. Available: https://www.techopedia.com/definition/5831/access-control. Accessed Sep. 1, 2016.

C. SECURITY THREATS IN CLOUD COMPUTING

The cloud computing security threats highlighted by Cloud Security Alliance (CSA) in its paper titled "Top Threats to Cloud Computing v1.0" [26] are shown in Figure 5. Incorporating the analysis of Barron et al. [27] on associated cloud computing attacks/threats with CSA's input, Table 5 presents a summary of the top seven security threats from some real-life case studies. The sections that follow elaborate on each of these threats.

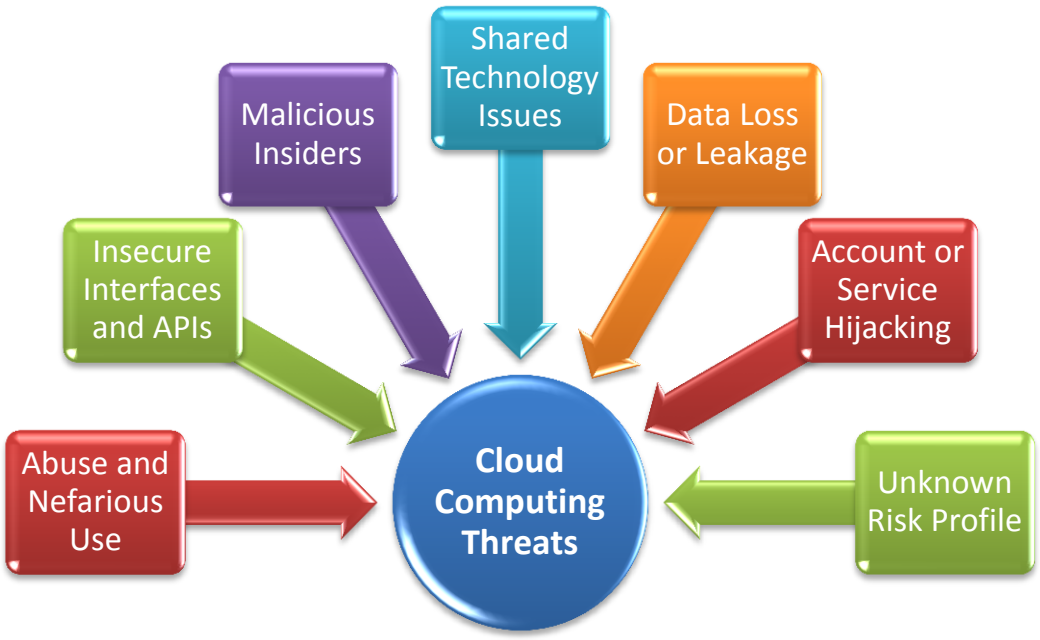


Figure 5. Security Threats in Cloud Computing. Adapted from [26].

Table 5. Cloud Computing Security Threats. Adapted from [26].

Threat	Description	Examples	Impact	Remediation
1. Abusive and Nefarious Use	Criminals are able to conduct their activities with easy and "unlimited" access to cloud resources	Cloud have hosted Zeus botnet, and downloads for exploits	Criminals are able to leverage on the cloud to improve their reach, avoid detection and continue to work on their activities	Stricter registration and validation process to gain access to cloud resources; Enhanced credit card fraud monitoring
2. Insecure Interfaces and APIs	Cloud providers usually provide a set of software interfaces or APIs for customers to manage and interact with their services	Anonymous access using compromised passwords; Clear-text authentication or transmission of content	Weak set of APIs can expose users to security issues relating to the C-I-A triad	Ensure that encrypted transmission, strong authentication, and access controls are implemented
3. Malicious Insiders	Insiders (e.g., cloud provider) can access and "steal" sensitive information stored in the cloud	No public example	Brand damage, financial impact, and productivity losses	Specify human resource requirements as part of legal contracts, etc.
4. Shared Technology Issues	Shared cloud resources (e.g., CPU caches, OS, etc.) are usually not designed to offer strong isolation for different users	Rutkowska's "Blue Pill" exploits [28]; Kortchinsky's CloudBurst presentations [29]	From the exploit of one operating system in the cloud, attackers would be able to gain access to unauthorized data stored for other cloud users	Enforce service level agreements for patching and vulnerability. Implement security best practices for installation/ configuration
5. Data Loss or Leakage	Data loss or leakage can happen in many different ways	Insufficient authentication, authorization, and audit controls; Inconsistent use of encryption and software keys; Operational failures; etc.	Brand and reputation; Partner, and customer morale and trust; Loss of core intellectual property; etc.	Implement strong API access control; Encrypt and protect integrity of data in transit; etc.
6. Account or Service Hijacking	Account or service hijacking using methods such as phishing, fraud, and the exploitation of software vulnerabilities	No public example	Attackers compromising the confidentiality, integrity and availability of the cloud services	Prohibit sharing of account credentials between users and services. When possible, leverage on two-factor authentication methods
7. Unknown Risk Profile	No or insufficient access to systems, network and application logs may lead to unknown risk profile for an organization	Despite the breach into U.S. Heartland's system, Heartland did not notify every single customer, about whether their data has been stolen	Unknown risk profile that may lead to serious consequences	Disclosure of systems, network and application log; Monitoring and alerting on sensitive information stored in the cloud

1. Abusive Use

Cloud users usually assume that the cloud resources such as computing power, storage space and network resources are unlimited. Hackers and cybercriminals can gain access to this unlimited resource simply through a registration process using a valid credit card. On this note, a "valid" credit card can also be a stolen or lost card, which in this case, hides the identity of the attacker. In addition to the easy registration process, limited, free trial periods may be offered by some cloud providers.

Cybercriminals, who access cloud resources with relative anonymity, are able to leverage the cloud's "new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities." In this context, cases of cloud hosting "Zeus botnet, downloads for Microsoft Office, and Adobe PDF exploits" were reported [26].

Cloud providers with weak registration processes are continuously being targeted as they offer cybercriminals relatively "free" access to unlimited cloud resources. Implementing stricter registration processes, enhancing credit-card fraud monitoring, as well as monitoring customer and publically blacklisted networks are some ways to mitigate cybercriminals' abuse of cloud computing [26].

2. Insecure Interfaces and APIs

Cloud users usually interact with cloud services via a set of software interfaces or application program interfaces (APIs). [10] While these interfaces provide for good provision, management, orchestration, and monitoring of cloud services for customers, cybercriminals can take advantage of these interfaces to conduct illegal activities. Cloud-based users may be exposed to security issues related to the C-I-A triad, if the used services are built upon a weak set of interfaces [26].

Attackers gaining anonymous access with reusable passwords or tokens and sniffing traffic with clear-text authentication tokens or data are examples of this threat on

[10] An application program interface (API) is a set of routines, protocols, and tools for building software applications. An API specifies how software components should interact, and APIs are used when programming graphical user interface (GUI) components, paraphrased from Application Program Interface. (n.d.). *Webopedia*. [Online]. Available: http://www.webopedia.com/TERM/A/API.html. Accessed Sep. 1, 2016.

insecure interfaces and APIs used by cloud providers. Cloud users can safeguard themselves by ensuring that proper authentication, encryption and access controls are being implemented in the cloud-based services [26]. Recently, in August 2016, Michael Osterman, president and founder of Osterman Research,[11] highlighted in his online brief that the privacy, compliance, and security challenges that Office 365 has faced in the cloud environment may "be addressed through the use of end-to-end encryption for all emails and files sent to Office 365" [30]. Moreover, with an understanding of the dependency chain associated with the interfaces and API, customers can decide—by determining the vulnerability of the interfaces—whether to do business with a given cloud provider [26].

3. Malicious Insider

Insiders (i.e., cloud provider employees) can have a significant impact on organizations' data stored in the cloud. This is primarily due to their uncontrolled level of access (required for work purposes) into an organization's assets. With such uncontrolled and unauthorized access into an organization's information, improper disclosure of information from insiders may lead to devastating consequences such as brand damage, financial impact, and productivity loss [26].

To mitigate insider threats, consumers can state human resource requirements in legal contracts. This will indicate exactly who is authorized to access what data [26]. Consumers should also ask for transparency into a cloud provider's overall security management of information in the cloud. Last, by "understanding and determining the security-breach notification process," consumers will be in a better position to guard themselves from insider threats [26].

[11] "Osterman Research conducts surveys on IT-related issues with both IT professionals and end users. Surveys focus on messaging management, instant messaging, messaging threats, backup and archiving strategies, operating system issues and other IT-related issues," quoted from Services. (n.d.). Osterman Research. [Online]. Available: http://www.ostermanresearch.com/services.htm. Accessed Sep. 1, 2016.

4. Shared Technology Issues

According to [26], cloud providers (specifically IaaS vendors) deliver their scalable services by sharing cloud infrastructure for different consumers. The underlying components (e.g., central processing unit caches and graphics processing units) that make up this infrastructure were never designed to offer strong isolation between different consumers. With a successful exploit on one system component in the cloud, an attacker may also gain access to unauthorized data in other—shared—cloud components operating in the same cloud infrastructure. Examples of such attacks are the Blue Pill, as discussed by Rutkowska in [28], and the CloudBurst, mentioned by Kortchinksy in [29], both of which targeted the virtualization technology shared in the cloud.

To mitigate the security issues related to shared technology, cloud providers should follow security best-practices for installing and configuring software and tools. Cloud providers can also improve their security posture by actively monitoring the cloud environment for unauthorized activities and taking necessary actions in the event of an intrusion. Additional methods for further reducing and possibly preventing attacks in the domain of shared cloud infrastructure include implementing strong authentication and access control, and conducting security audit scans at suitable time periods [26].

5. Data Loss or Leakage

Data loss or leakage can happen in many different ways. Some examples include insufficient authentication, authorization, and audit controls; and unauthorized access to sensitive data. Data loss or leakage from cloud services can have severe impacts on a business: reduced morale and trust among employees, partners, and customers; “damage to brand and reputation”; “compliance violations” resulting to legal actions [26].

Thus, it is important for cloud providers to ensure that security measures are taken to mitigate any loss of data. Examples of such security measures include “implementing a strong and robust API access control; implementing strong key generation, storage and management, and destruction practices; and encrypting and protecting the integrity of data during transmission” [26].

6. Account or Service Hijacking

Cybercriminals can hijack accounts and services with stolen credentials through social engineering attacks. This gives them access to sensitive areas, which position them to compromise the C-I-A of the cloud services. Attackers can also choose to reuse any compromised credentials, enabling them to conduct various attacks over a time span that is convenient for the attacker—and less likely to be detected. Such a long-term, persistent presence may ultimately lead to the attacker achieving full command and control (C2) over many cloud service subscribers' machines (i.e., computers, systems, and hosts) [26].

Therefore, it is important for organizations to implement defense-in-depth protection strategies (multiple layers of mutually supportive security controls), and follow the principle of least privilege (personnel and machines are given minimal access rights/privileges to perform their necessary work, and nothing more) to contain the harm resulting from a breach of an individual account or service. By "prohibiting the sharing of account credentials between users and services, leveraging strong two-factor authentication techniques, and employing proactive monitoring to detect unauthorized activity" [26], the cloud provider can reduce the impact from any hijacking. Two illustrative examples of account or service hijackings follow:

a. The Hijacking of Matthew Prince's Personal Gmail Account

In 2012, the hacker group UGNazi exploited flaws in Google's and AT&T's password recovery process and voicemail system, respectively, to gain unauthorized access to CloudFlare CEO Matthew Prince's personal Gmail account. Prince [31] has named four critical security flaws that allowed the incident to occur:

1. AT&T was tricked into redirecting my voicemail to a fraudulent voicemail box;
2. Google's account recovery process was tricked by the fraudulent voicemail box and left an account recovery PIN code that allowed my personal Gmail account to be reset;
3. A flaw in Google's Enterprise Apps account recovery process allowed the hacker to bypass two-factor authentication on my CloudFlare.com address; and

4. CloudFlare BCCing transactional emails to some administrative accounts allowed the hacker to reset the password of a customer once the hacker had gained access to the administrative email account. [31]

b. Social Engineering Attack

"A social engineering attack is an intrusion that relies heavily on human interaction, often tricking people to break normal security procedures" [32]. (See Figure 6.) This happens not only in traditional client-server systems but also in cloud computing.

Figure 6. Life Cycle of a Social Engineering Attack. Adapted from [33].

In August 2012, hackers were able to use flaws in the identity verification systems used by Amazon and Apple to remotely erase information from technical writer Mat Honan's Apple devices (i.e., iPad, MacBook, and iPod) [27]. With alignment to the life cycle of a social engineering attack (see Figure 6), the following describes the incident in a chronological order:

- Step 1 (Identify Target) – The hacker identified Mat Honan as a potential target in this step.
- Step 2 (Search Information on Target) – The hackers searched information on Mat and found his @me.com address online. This provided the hackers with information that there was an associated AppleID account.

- Step 3 (Identify Vulnerabilities in Business Process and Human Resources) – Knowing the vulnerabilities in business processes and human resources, the hacker exploited them.

  The hacker first called the customer service of Amazon to add a new credit card number to Mat's account. Amazon's verification process required the hacker to provide "information such as the name, billing address, and associated email address" on Mat's account, which the hacker had already obtained online. After answering the questions successfully, Amazon's representative added the new credit card information to Mat's account [27].

  "Ending the call, the hacker called Amazon's customer service again and reported that he had lost access to his account." For a new email address to be added to Mat's account, the hacker needed to provide Mat's "billing address and the credit card associated with the account—the hacker used the new credit card information he provided from the previous phone call)" [27].

  With the newly added email, the hacker requested a password reset for Amazon's website. "The hacker now had access to Mat's Amazon account and credit card information on file."

  "The hacker, then, called Apple technical support and requested a password reset on the Mat's @me.com email account. Although the hacker did not manage to answer any of the victim's account security questions, Apple offered him another option. The Apple representative only required a billing address and the last four digits of the victim's credit card to issue the hacker a temporary password" [27].

- Step 4 (Achieve Objective of Attack) – With the "temporary password, the hacker had access to the victim's Apple iCloud account. All the information from the victim's iPad, MacBook, and iPod account was remotely erased" [27].

- Step 5 (Eliminate evidence of attack) – Given the detailed information pertaining to the incident, the attacker did not manage to eliminate traces of his attack. Nevertheless, the attacker did well hiding his identity after meeting the objective.

7. Unknown Risk Profile

The main reason why organizations are adopting cloud computing is that it reduces hardware and software ownership and maintenance costs, thus allowing companies to focus more on their core businesses. Analysis in Cloud Security Alliance's report showed obvious financial and operational benefits, however, "such benefits must

be weighed carefully against the countervailing security concerns" [26]. The features and functionality of the cloud may be very well described and explained, it is equally important to know "the internal security procedures, configuration hardening, patching, personnel access, auditing, and logging controls" implemented by the cloud service provider. These, however, are often "overlooked, leaving customers with an unknown risk profile" [26].

Thus, it is important for cloud users to request relevant logs and data (e.g., system, network, and application logs) and infrastructure details (e.g., patch levels and firewalls) from the cloud provider, to put them in a better position to determine their security posture [26].

D. SECURITY MINDSET

Traditional—though wrongheaded—thinking is that if there is no connection between a particular system and the Internet, the system is safe from external attacks. This mindset may be one reason why sensitive organizations, such as those in the government and defense sectors, continue using their traditional "local" systems that maintain all data and services in-house (i.e., locally provisioned), instead of switching to the cloud.

This mindset—that systems without connectivity to the Internet are not vulnerable to attacks—is problematic. For example, Stuxnet, a malicious computer worm, exploited four zero-day[12] flaws in a system that had no direct connection to the Internet [34]. In another example reported by the British Broadcasting Corporation (BCC), Flame, a form of malware, attacked another system without exploiting connectivity. A report by Professor Alan of the Department of Computing at the University of Surrey described Flame as similar to Stuxnet, which has the capability to spread by USB stick [35].

A local system without connectivity to the Internet can be either as secure or as vulnerable as one that is connected to the Internet, depending on situation. Although it is

[12] "A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack," quoted from What Is a Zero-Day Vulnerability? (n.d.). PC Tools by Symantec. [Online]. Available: http://www.pctools.com/security-news/zero-day-vulnerability/. Accessed Sep. 1, 2016.

difficult to change the mindset of people, it is important for them to recognize that a local system without connectivity to the external network (i.e., the Internet) can also be vulnerable to attacks. Thus, it may be worthwhile to switch to cloud computing, which provides similar functionalities at a lower cost.

E. SUMMARY

This chapter discussed the three information security objectives: confidentiality, integrity, and availability. These objectives are equally applicable to cloud-based information systems as they are to traditional, non-cloud-based systems. With these security objectives in mind, we identified and described the top seven security threats to cloud-based services. We also discussed the security mindset at play in preventing some organizations from switching to cloud computing. Chapter VI examines cloud features deemed essential for best supporting the needs of the SAF operations and then recommends a suitable cloud migration framework for the SAF's transition into cloud computing.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDED CLOUD ADOPTION POLICY FOR THE SAF

A. OVERVIEW

As discussed in earlier chapters, cloud computing has enabled IT systems to be easily scaled up or down for operational use in sectors such as healthcare, business, and defense. Organizations no longer need to decide their exact hardware and software requirements up front. Instead, they can use computing resources based purely on demands. Using the services provided by cloud computing, an organization can run its operations without the need to purchase physical hardware, which results in the organization reflecting huge savings.

Chapter V discussed the meaning of information-security as it relates to cloud computing, including various examples of threats and the mitigations thereof. This chapter explores the cloud "features" needed for Singapore Armed Forces (SAF) operations. Then, with the specific features in mind, suitable cloud adoption policy recommendations are offered that should help guide the SAF's transition to cloud computing. These recommendations include guidance based upon the cloud security requirements found in documents from the Cloud Standards Customer Council (CSCC) and the National Institute of Standards and Technology (NIST).

B. MILITARY COALITION OPERATIONS

At the heart of a military's operational effectiveness is its command and control (C2). Even a military with advanced systems and technologies will not function effectively if the C2 between its headquarters and various executing units is weak. In other words, if commands from headquarters fail to reach the tasked unit or are unclear, the tasked action unit will be unable to execute the mission as expected by headquarters.

In addition to C2, the integrity, accuracy, and relevancy of commands/instructions also play a significant part in the successful conduct of military operations. For example, after identifying an enemy's hideout location, headquarters may instruct the designated units to attack the identified location. However, if the information provided is no longer

timely/accurate (e.g., the enemy has left the previously reported location), that message will not aid in the success of the mission.

Effective operations in the military require considerable coordination among different branches (e.g., human resources, intelligence, and logistics). While it may seem complicated, the processes involved can be summed up easily using the Observe, Orient, Decide, and Act (OODA) loop model (see Figure 7). The OODA loop, developed by U.S. Air Force Colonel John Boyd, is a decision cycle for the purpose of information warfare [36].

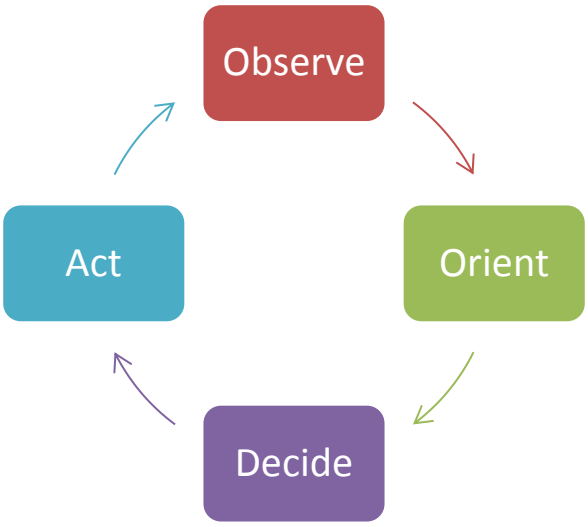


Figure 7. OODA Loop. Adapted from [37].

According to Boyd, the faster that a military unit can cycle through the ever-repeating OODA loop, the more efficient and effective its various operations will be [37]. Despite the OODA loop being well defined; Berndt Brehmer, a professor from the Department of War Studies at the Swedish National Defense College, emphasized that for a military force to be effective in its C2, the OODA loop needs to be formulated in terms of functions (i.e., asking C2 questions) [38]. Fortunately, the hard work of defining these functions was completed by the military historian Van Creveld in his book *Command in War*, in which he defined the following eight functions, which we treat as characteristics of effective C2:

- Gathering information about one's own forces, the enemy, as well as external factors such as weather and terrain
- Storing, retrieving, filtering, classifying, distributing, and displaying the gathered information
- Estimating the current situation
- Forming objectives and alternative methods for attaining them
- Making a decision, followed by detailed planning
- Drafting orders and transmitting them down to recipients
- Verifying that the recipients have understood the orders correctly
- Monitoring execution of orders by means of a feedback system, at which point the entire process repeats itself [39]

Using the fundamental concepts of the OODA loop in conjunction with Creveld's definition of the characteristics of effective C2, we now have the basic framework to articulate cloud features that are desirable in a military context. Such features should encompass SAF operations in all types of missions (e.g., humanitarian assistance and disaster relief [HADR] and coalition operations).

The main concept from the OODA loop is to leverage advanced technologies (e.g., computers, cloud processing, and sensors) to help commanders and soldiers cycle though the loop's stages quickly, thus outmaneuvering the enemy and putting ordnance on target more quickly and accurately. In addition, as a military force cycles through the OODA loop it is also important for it to answer all "C2 questions" defined by Creveld.

For example, the first C2 function of gathering information can be re-written as the following question: "*How* can the gathering of information about one's own forces, the enemy's forces, as well as external factors such as weather and terrain be achieved in a *fast* and *efficient* manner through the use of a cloud-based feature that benefits the military?" As such, the following are recommended cloud features for a military force:

1. Intelligence through Live Sensors

In order for the cloud to support a military force, its services must be able to gather intelligence (e.g., information pertaining to its own forces, enemy forces, as well

as external factors such as weather and terrain) for the unit, not only in a fast and efficient manner but also in a format easily understood by its users. For example, we can use live sensors (e.g., unmanned aircraft, cameras, and weather equipment) to gather the raw data (e.g., pictures and temperature) and, then, automatically display the information in a format readable by humans. In this manner, commanders can focus their time developing strategic plans instead of processing the raw data manually.

2. Intelligence System

In addition to gathering and displaying intelligence information, the cloud service must have the ability to process the gathered information, filter unnecessary data, as well as classify and distribute the information to relevant users. This can take the form of alerts to various users on the arrival of new information, which can have a significant impact on the mission. Furthermore, the cloud service should also be able to generate status reports (e.g., manpower and logistics) based on the updated information gathered.

3. Current Situation Picture

The most difficult part about a mission is "painting" the current situation during operations; a battle is very dynamic, constantly changing with every decision made by a commander and every action made by a soldier. To help the SAF in such a situation, the cloud service should be able to provide a near real-time "picture" in the form of a map. This map shows locations of its own forces (e.g., using GPS technology and feedback from the ground) as well as enemy forces from intelligence gathered, and facilitate military commanders with the ability to efficiently assess the situation and make accurate decisions.

4. Planning and Collaboration Tools

For a military to function, commanders need tools to aid them in their planning and collaboration with other branches (e.g., HR, intelligence, and logistics) and services (e.g., army, navy, and air force). According to Robert R. Leonhard, a member of Applied Physics Laboratory's Principal Professional Staff in the National Security Analysis Department, planning tools (e.g., map planning) in the military have previously lacked

the kind of automation that could help commanders identify capabilities and weaknesses of both their own and enemy forces. Leonhard also highlighted that collaborations, both vertically and horizontally, must be facilitated in order for effective C2 to happen [40].

5. Effective Transmission Medium

We would expect any "cloud-based" service to be "carried" over an effective transmission medium since it is, or can be, interconnected to the global Internet. The inherent connectivity should facilitate the quick and reliable exchange of data from one location to another. This is in contrast to many military communication systems (e.g., terrestrial radios, satellite communications, etc.) wherein the reach is limited to the actual footprint of the systems dedicated to the specific operation/network. Therefore, a cloud-based network will be a better choice when global "reach" using already existing infrastructure is considered an advantage. As an example, Singapore's participation in a country-level joint operation (e.g., for HADR) will require communication and collaborations with other countries situated geographically far away. It may be difficult for any military force, using their own organic communications gear, to extend their communication network to include all participating countries. Furthermore, the communication devices and systems from each country may be rather non-standardized, and thus not easily interoperable with one another. Thus, a secure cloud service is the ideal "application" and transmission medium for countries to collaborate.

Referring back to the functions/questions, with the cloud being the transmission medium to send orders to tactical action units, the cloud should also contain a feature to verify that the action units have received and understood the orders correctly.

6. Monitoring

As important as intelligence gathering is, the cloud service should also be able to monitor the execution of orders (e.g., units attacking an objective, and artillery battle damage assessments) by means of a feedback system. This feedback system will help commanders assess the effectiveness of the actions being executed.

7. Ability to Scale Up and Down

The desired list of C2 features/tools conducive to the conduct of effective military operations is ever changing and growing as new capabilities become available with advances in research and technology. Because cloud computing has the ability to scale up or down easily, it is the recommended platform/approach from which to support rapid adoption and hosting of new features/tools as they arrive on the market. Every day militaries are improving and evolving. These changes often entail the need to "communicate" and integrate with the core/main C2 systems, which indirectly requires additional services/features to be added into the cloud. Moreover, doctrine drives how a particular military runs. With each military defining its own doctrine uniquely, it is very difficult to define common terms that describe the precise cloud features necessary for every military. Thus, the aforementioned recommendations represent the basic cloud features any military would find desirable, if not necessary, in order to run its operations most effectively. Figure 8 illustrates the desired military cloud features listed above integrated in the OODA loop process:

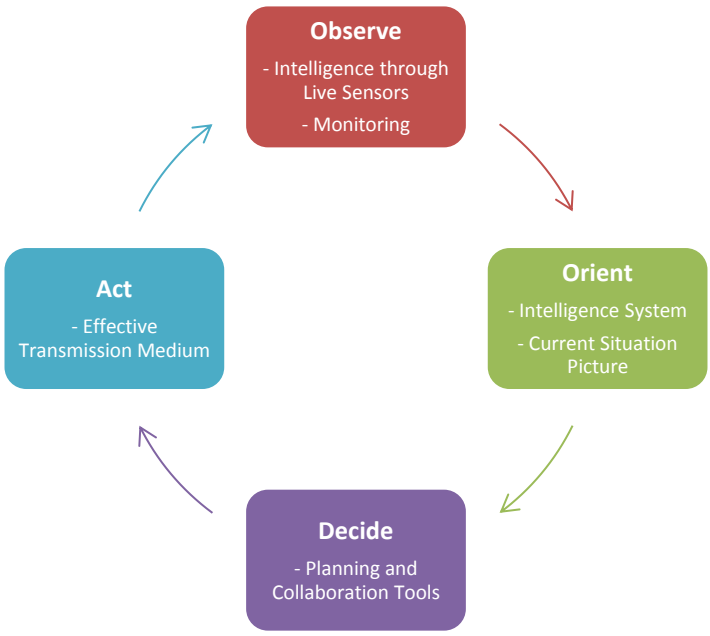


Figure 8. Basic Military Cloud Features Integrated into the OODA Loop Process. Adapted from [37]

C. DECISION FRAMEWORK FOR CLOUD ADOPTION

Even though cloud computing presents many "unknowns" for the would-be user, a step-by-step guide would aid the SAF's migration to the cloud environment. Fortunately, such a guide, titled "Migrating Applications to Public Cloud Services," already exists as developed by Cloud Standards Customers Council (CSCC) [41]. Although this guidance is not tailored specifically to the military community, many of the principles upon which it is based are universal in nature and thus applicable to any community. Differences, where there are any, are largely only a matter of degree. For example, all cloud users are likely to desire *some* degree of confidentiality for their data that resides on cloud servers, while the military user will likely *insist* on this! Figure 9, adapted from [41], shows a general framework for the SAF to move to the cloud:

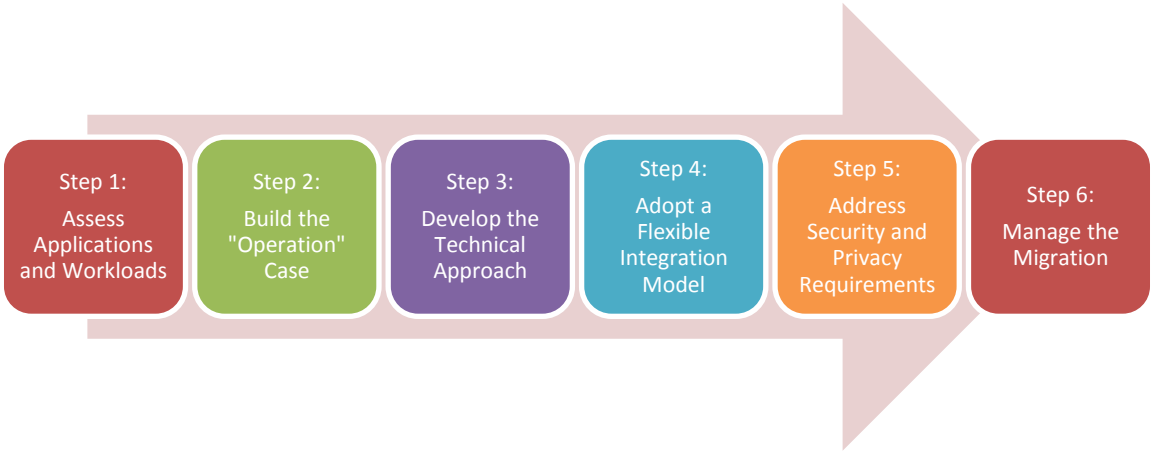


Figure 9. Migration Framework. Adapted from [41].

In Step 1, the SAF needs to analyze and assess the readiness (i.e., applications and workload) of the cloud services that it wants to engage. This would also include determining the cloud model(s); i.e., private, community, public and hybrid as elaborated upon in Chapter I, supported by the cloud provider. By doing so, the SAF will be able to determine the applications and data suitable for usage in the associated cloud environment.

Step 2 involves building an "operation case study" for each IT application migrating from a traditional system to the cloud. This case study will define the current situation and highlight the advantages that cloud computing provides for that particular application. Before the actual migration, it is important for the SAF to identify sufficient advantages that provably outweigh the continued use of traditional IT systems. Such a case study can include 1) Cost analysis; 2) Service Level of the Cloud; and 3) the SAF Operation Impact. Refer to [41] for examples and elaboration on the operational case.

In Step 3, the SAF decides and subscribes to the type of cloud service model (i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) as explained in Chapter I) that is most suitable for its mission requirements. Because each cloud service model has a different division of responsibilities (i.e., cloud infrastructure, platform and software) between the user (in this case the military) and the cloud provider, the user has to determine if it has sufficient people with the necessary technical skills to manage these responsibilities, before deciding on which service model to take. For example, if a military has insufficient IT talent, the most appropriate model would be SaaS, because that model entails the service provider providing the greatest degree of support in comparison to what is needed/expected from the customer.

Step 4 entails adopting a flexible integration model. Most of the time systems do not work or function in isolation, but instead require communication or "integration" with other systems for their inputs, outputs, and related capabilities and system dependencies. This is especially so for the SAF, with constant changes and improvements occurring. For example, an application in a system may need to invoke another application residing in another system in order for it to carry out the assigned tasking. Quoted from CSCC, the following are approaches for adopting a flexible integration:

> • be flexible, potentially including several different techniques according to specific situations
>
> • be based on standards, in order to be more maintainable and less fragile with respect to changes the cloud provider might make

• consider the possibility that more migrations may occur in the future—"therefore cloud migration is an opportunity to modernize the architecture and render it more resilient to such changes" [41].

In step 5, the SAF will address the security and privacy requirements of its cloud services. Security requirements includes asking questions like how difficult is it for hackers to get access to the restricted cloud data, and when that happens, will affected users be notified about it. Addressing privacy issues is similar to addressing security issues with the main difference being that a violation to privacy has occurred. This violation may have serious consequences such as damage to a military's reputation and legal actions taken [41]. The SAF should follow the logical steps listed in CSCC's "Security for Cloud Computing: Ten Steps to Ensure Success" [42], to mitigate security and privacy risks when using the cloud.

The last step 6, entails the execution and management of the migration of existing military IT systems into the cloud services. Like any other military project, it should consist of a project manager and team who are constantly tracking and overlooking its planned schedule, cost, resources and calculated risks. CSCC has provided yet another step-wise procedure to assist with this—the 6th step—of the migration framework (Figure 9) 6-step process. This procedure, consisting of five steps, quoted from [41], CSCC describes the management procedure steps thusly:

> Step 1: Deploy the Cloud Environment Provision. Install and test the necessary storage, compute, network and security resources that constitute the cloud environment in which the migrated application will run.
>
> Step 2: Install and Configure the Applications. The applications and supporting middleware should now be installed and configured on the cloud servers. Cloud service providers frequently do this through automated deployment of templates.
>
> Step 3: Harden the Production Environment. Install additional utilities for business continuity and security. Note that some of these services may be provided by the cloud service provider, in which case they do not need to be installed, but they should still be tested.
>
> Step 4: Execute a Mock Migration. Undergo a trial run of the migration project plan to uncover unintended results or unnoticed issues during the planning phase. The mock migration date should be sufficiently distant

from the desired final cutover date to have time to rectify problems. Involve the cloud service provider in the migration date selection.

Step 5: Cutover to Production Cloud. Assuming a successful mock migration, or one that only encountered minor issues with a clear fix, establish a formal cutover schedule. If the mock migration ran into serious issues, then it needs to be repeated after correcting the causes. [41]

D. SECURE CLOUD-BASED FRAMEWORK/GUIDELINES

After defining the systematic decision framework for cloud adoption, the SAF would also need a security framework/guidelines to implement a *secure* cloud environment for use in operations. In March 2016, DISA developed a cloud computing security requirement guide (SRG) titled "DEPARTMENT OF DEFENSE CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE Version 1, Release 2" [43]. Release 2 is a revised version that includes information on handling more sensitive data. In the SAF's context, this data is referred to as "*restricted* and above" information. With reference to this security requirement guide, subsequent sections explain the secure cloud-based framework/guidelines in the context of the SAF.

Table 6 summaries the potential impact definitions for information security (explained in Chapter V). The SAF can use this guide to classify the impact level of a given system, and then implement the necessary security requirements shown in Table 7. The 'A' (availability) of the C-I-A triad is not included in the Table 6 impact definitions, because the client, or what the CSCC refers to as "mission owners",[13] are expected to assess the availability during the *selection* of a cloud service provider. Cloud service clients have to specify the availability requirement in the contract. For example, a cloud service provider may be asked to provide a minimum one-week advance notice before performing any maintenance that may affect the availability of the cloud-based services. Clients may also insist on various degrees of data duplication; e.g., data-mirroring, archiving, and alternate geographic site storage redundancy.

[13] Mission owner refers to the entity responsible for the contracted cloud-based services. Examples of such entity include IT system owner or unit officer (e.g., unit commanding officer) leveraging on a cloud service provider's services in completing a mission.

Table 6. Potential Impact Definitions for Information Security. Source: [43]

Security Objective	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 7, adapted from [43], provides a summary of the security requirements mapped to the information impact characterizations enumerated in Table 6. The content of the original table cells have been modified to reflect a more SAF-centric view.

Table 7. Summary of Information Sensitivity with Associated Security Requirements. Adapted from [43].

Information Sensitivity	Security Control	Location	Off-Premise Connectivity	Separation	Personnel Requirements
Non-Controlled Unclassified Information (SAF: Unclassified)	SAF Security Control Level 1	SAF off premise or SAF on premise location	Internet	Virtual/Logical PUBLIC COMMUNITY	Personnel (i.e., soldiers and employees) of the SAF
DISA SRG Level 4 Controlled Unclassified Information (SAF: Restricted)	SAF Security Control Level 2	SAF off premise or SAF on premise location	SAF Homeland Defense Network	Virtual/Logical SINGAPORE HOMELAND SECURITY COMMUNITY	Personnel with minimum military CAT 2 cleared
DISA SRG Level 5 Controlled Unclassified Information (SAF: Restricted)					

Information Sensitivity	Security Control	Location	Off-Premise Connectivity	Separation	Personnel Requirements
Classified Information up to SECRET (SAF: Confidential and Secret	SAF Security Control Level 3	SAF off premise or SAF on premise location (Locations must be equipped with cleared/classified facilities)	SAF Classified Network (CLASSNET)	Virtual/Logical SINGAPORE ARMED FORCES COMMUNITY	Personnel with military CAT 2A clearance can work with confidential information Personnel with military CAT 1 clearance can work with secret information

1. Information Sensitivity

Non-controlled unclassified information refers to data that are cleared for public release; the SAF refers to this information as unclassified information. Changes to this information would require access control. This category accommodates information with impact level up to low confidentiality and moderate integrity (see Table 6).

In the DISA SRG [43], the definition of level 4 controlled unclassified information (CUI) does not include classified information, but a law or a regulation controls the handling of such CUI [44]. However, the SAF *did* classify this information as being restricted. Whichever terminology are being used, this category refers to data that are more sensitive and require a higher level of access control. Examples of information in this category include privacy information such as a personal identification number, bank account number, or home address; in which companies/entities need to abide by the rules of the Personal Data Protection Act when handling citizens' data in Singapore. This category accommodates information with impact level up to moderate confidentiality and moderate integrity (see Table 6).

The DISA SRG's definition of level 4 and level 5 (includes national security systems) CUI seems to match what the SAF define as "restricted." For this purpose, the security requirements for SAF's restricted information will be matched to the "stricter" DSIA SRG's level 5 CUI being defined. Similarly, this category should only

accommodate information with impact level up to moderate confidentiality and moderate integrity (see Table 6).

Last, classified information up to secret includes information defined as confidential and secret for the SAF. SAF information classified as secret and below (i.e., unclassified, restricted, confidential or secret) is included in this level. This category also accommodates information with impact level up to moderate confidentiality and moderate integrity (see Table 6).

The DISA SRG did not specifically explain the handling of top-secret information using cloud-based services. However, in Oct 2014, James Cook, a reporter from Business Insider, reported that DOD has the intention to move top-secret information into the cloud environment [45].

2. Security Control

From the DISA SRG, different security control methods or guidelines were used for different cloud-based services, primarily based on the sensitivity level of the information the services would process or store. NIST Special Publication 800–53 [46], "Security and Privacy Controls for Federal Information Systems and Organizations," and the "Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework v2.1"[14] [47] were referenced to provide the security controls necessary for cloud-based services.

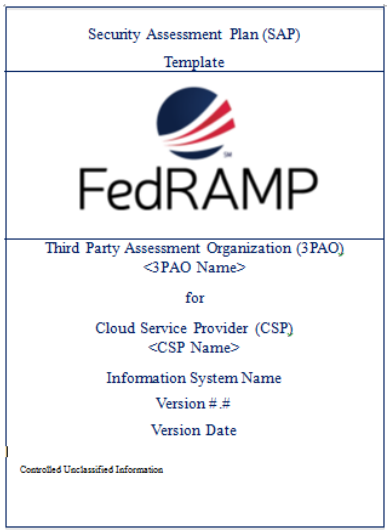
The following describe in detail the requirements for each security control guideline shown in Table 7:

[14] "FedRAMP is a U.S. Government program to standardize how the Federal Information Security Management Act (FISMA) applies to cloud computing services," quoted from the National Institute of Standards and Technology. (2015, Dec). FedRAMP security assessment framework. DOD. [Online]. Available: https://www.fedramp.gov/files/2015/01/FedRAMP-Security-Assessment-Framework-v2-1.pdf. Accessed Sep. 9, 2016.

a. SAF Security Control Level 1 (for Unclassified Information)

Cloud service providers who are interested in providing services to the SAF must meet the "SAF security requirements" and implement the "SAF baseline security control."

To meet the SAF security requirements, a cloud service provider has to engage an independent and technically competent[15] third-party to assess its security position, and then, complete a security assessment plan (using FedRAMP security assessment plan template as a recommendation [see Figure 10]) developed by the third-party assessor.



"This document, released originally in Template format, is designed for" cloud service provider "third-party independent assessors to use for planning security testing of cloud service providers" [48]. See [48] for the entire document.

Figure 10. FedRAMP Security Assessment Plan Template. Source: [48].

The baseline security control for cloud-based services storing unclassified information has to fulfill the following: 1) implementation of access control such as "unsuccessful login attempts" and "principle of least privilege"; 2) security awareness and training for cloud users; 3) perform audits at suitable time period; 4) security assessment and authorization; and more. This is equivalent to "FedRAMP compliant

[15] A security assessor who meet the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17020 standards is considered technically competent.

at the moderate level" (see "FedRAMP Low Moderate System Security Plan Template" of [48]).

b. SAF Security Control Level 2 (for Restricted Information) and Level 3 (for Information up to Secret)

On top of the SAF security controls for level 1, level 2 includes some additional controls that address security issues, such as advanced persistent threats and insider threats. These additional requirements, in abbreviated format, are indicated in Table 8.

Table 8. Summary of Information Sensitivity with Associated Security Requirements. Adapted from [46].

SP 800–53r4 Control ID (See [46]**for details)**	**SAF Security Control Level 2**	**SAF Security Control Level 3**
AC-06 (07)	X	X
AC-06 (08)	X	X
AC-17 (06)	X	X
AC-18 (03)	X	X
AC-23	X	X
AT-03 (02)	X	X
AT-03 (04)	X	X
AU-04 (01)	X	X
AU-06 (04)	X	X
AU-06 (10)	X	X
AU-12 (01)	X	X
CA-03 (01)	X	X
CM-03 (04)	X	X
CM-03 (06)	X	X
CM-04 (01)	X	X
CM-05 (06)	X	X
IA-02 (09)	X	X
IA-05 (13)	X	X
IR-04 (03)	X	X
IR-04 (04)	X	X
IR-04 (06)	X	X
IR-04 (07)	X	X
IR-04 (08)	X	X
IR-05 (01)	X	X
IR-06 (02)	X	X
MA-04 (03)	X	X
MA-04 (06)	X	X
PE-03 (01)	X	X
PL-08 (01)	X	X
PS-04 (01)	X	X
PS-06 (03)	X	X
SA-04 (07)	X	X

SP 800–53r4 Control ID (See [46]for details)	SAF Security Control Level 2	SAF Security Control Level 3
SA-12	X	X
SA-19	X	X
SC-07 (10)	X	X
SC-07 (11)	X	X
SC-07 (14)	-	X
SC-08 (02)	X	X
SC-23 (01)	X	X
SC-23 (03)	X	X
SC-23 (05)	X	X
SI-02 (06)	X	X
SI-03 (10)	X	X
SI-04 (12)	X	X
SI-04 (19)	X	X
SI-04 (20)	X	X
SI-04 (22)	X	X
SI-10 (03)	X	X

The main difference between SAF security control level 2 and 3 is that "SC-07 (14)," defined as "BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS," is not required for level 2 security control [46].

3. Location

The requirement for "SAF off premise locations" refers to locations within Singapore, excluding the SAF-related entities such as camps and headquarters. When this is mentioned for a non-SAF cloud provider, the provider would have to maintain the physical storage of SAF data within Singapore. The main objective of this is to protect against improper seizure and use by persons or organizations in other countries.

In contrast, "SAF on premise locations" refers to SAF's infrastructures (e.g., buildings, camps and more) with proper physical access controls being implemented for authorized entry.

In the context of the SAF, locations with "cleared/classified facilities" refers to locations with 1) access control for authorized entry; 2) at least two keys required for entry-one for unlocking and the other for dis-alarming; and 3) an alarm system mechanism implemented.

4. Off Premise Connectivity

While the Internet serves as good coverage in terms of connectivity for SAF operations, it is important to have different networks to support cloud-based services that process data with different levels of sensitivity. As per what the SAF has implemented, the existing homeland defense net will provide connectivity for cloud-based services with restricted data, allowing communication to occur between SAF and homeland security partners such as the police, fire, and medical departments. The CLASSNET,[16] which provides network connectivity to entities (e.g. DSTA and more) the SAF communicates with more often, will continue to be used for cloud-based services processing or storing data sensitivities from above restricted up to and including the secret level. However, "restricted" data may also be transmitted in this network.

5. Separation

Similarly, based on the likelihood of data with different sensitivity levels residing in cloud-based infrastructure, certain physical or logical separation has to be implemented. For example, cloud infrastructure that stores, processes, or transmits secret data will require separation controls to help ensure that such information does not, accidentally or via malicious machinations, spill outside of the SAF secret enclaves/networks.

6. Personnel Requirements

Currently, the SAF has a process of assigning security clearance status (i.e., CAT 1, CAT 2 and CAT 2A) to its personnel. A security clearance status would give its holder permission to access a piece of information (or more generically, an "object") categorized (or "labeled") to a particular sensitivity level. For example, an individual with a military CAT 1 clearance would have access permission to handle information up to and including the secret level.

[16] SAF Classified Network (CLASSNET) is a network built using IT resources, physically separated from other networks in terms of connectivity. The purpose of having a physically separated network is to prevent any potential leak of sensitive data from this network to other networks.

E. RECOMMENDED POLICY STATEMENTS

This section aims to provide high level policy guidance for the SAF's adoption of cloud-based computing. This comes in the form of policy statements that define basic, best-practice precepts that should be considered when considering whether to adopt a cloud-based computing solution for any particular SAF need.

1. Policy Precepts

The following policy statements are recommended based on the research presented here along with this author's approximately 10-years of experience as a signal officer in the SAF. While it is a desired outcome for the SAF to leverage the advantages afforded by cloud-based computing, there is no expectation on the part of this author that these statements of policy will necessarily be turned into official SAF policy. The intention here is to, at a minimum, "get the ball rolling" with regard to the SAF's adoption of cloud-based computing.

The recommended policy statements are articulated in the context of SAF operations that are likely to be supported by the adoption of cloud-based computing. To this end, much of the terminology used is as described earlier in Section D of this chapter.

2. Format

The format for each policy statement includes: 1) the policy statement itself, 2) a list of sections from the DISA SRG or other documents that was used as the reference source for the policy statement, and 3) a short "discussion" paragraph where supporting commentary regarding the rationale for the statement can be addressed.

3. Policy Statement 1

Statement: SAF systems handling unclassified information can adopt public cloud-based services.

Reference(s): Systems handing unclassified information (see Table 7 and Section 3.2 of [43]) or data that are cleared for public release can adopt public cloud-based services. This is mainly because losing information in this category results to (at most)

low impact to confidentiality and moderate integrity (see Table 6) which is not catastrophic.

Discussion: It is considered safe for the SAF to start adopting cloud computing to host the information found in its public domain websites. Examples of such website include the ministry of defense (https://www.mindef.gov.sg/imindef/home.html) and national service portal (https://www.ns.sg/nsp/portal/mindef/mindef-nsmen), of which both contain only information up to unclassified or public release.

4. Policy Statement 2

Statement: SAF should have a more stringent assessment (via a third party) for cloud service providers who wish to provide cloud-based services storing or processing higher-level sensitive data.

Reference(s): It is important for the SAF/mission owner to assess cloud-based services correctly, meeting the associated security control (see security control column of Table 7) before signing contract with a cloud provider. In addition, a third party organization is required to plan and conduct the assessment for the SAF [47].

Discussion: The SAF should ensure different assessment criteria for cloud-based services that are expected to host information spanning more than one sensitivity level. As shown in Table 7 and explained in Section D-2 of this chapter, cloud-based services comprised of higher-level sensitive data would result to a more stringent assessment. This is necessary because higher-level sensitive data requires more protection to help ensure that such information does not, accidentally or via malicious activities, spill outside of the associated network. To achieve this, the data owner (SAF in this context) should contract with an organization/vendor that is qualified to conduct information/cyber security assessments of any candidate cloud provider. The data owner is then positioned to either approve, or not, the cloud provider based upon the results. Any such third party assessment organization/vendor must demonstrate independence, objectivity, and the technical competence required to assess the security posture of cloud-based service providers.

5. Policy Statement 3

Statement: Physical cloud computing resources must be properly stored based on the sensitivity level of information they process or store.

Reference(s): Consolidated physical cloud IT resources should be properly stored based on the sensitivity level of information they process or store (see Table 7, and Sections 4 and 5.6 of [47]).

Discussion: It was explained in earlier chapters that the consolidation of IT resources via adoption of cloud computing, can help to significantly reduce hardware maintenance and IT staff cost. However, the cloud infrastructure should be properly located and "housed so as to protect the various devices against various threats. The SAF's current operating procedures of storing physical IT resources in physical compartments that are locked (2 different keys are required to open), alarmed-enabled, and located within SAF's greater protected infrastructure, should also be continued for a cloud computing environment. Continuing this practice, which also fulfills the requirements stated in Table 7, would help mitigate risks against physical seizure and insider threats of cloud-based computing.

6. Policy Statement 4

Statement: Appropriate cloud connectivity must be used for cloud-based services comprised of different level of data.

Reference(s): The "Off-premise connectivity" column of Table 7 and Section D-3 of this thesis provides details and explanation of the connectivity requirements for cloud-based services comprised of different level of information.

Discussion: Cloud-based services comprised of sensitive information will require a secured network, with physical connectivity that is separate from networks carrying information classified at lesser sensitivity levels. This is intended to help mitigate the risk of higher-level information leaking into a system that is not sufficiently secure to protect that (higher) level of information. In the context of the SAF, this means that cloud infrastructures used for the SAF CLASSNET should not be physically connected to the

homeland defense network, and the homeland defense network should not be physically connected to the Internet.

7. Policy Statement 5

Statement: Cloud-based services must be able to provide any required virtual/logical separation-enforcement when different communities are likely or known to share cloud infrastructure.

Reference(s): Virtual/logical separation capability must be available in cloud-based services when different communities (i.e., public, homeland security and SAF) share at least some portion of cloud infrastructure. The "Separation column" of Table 7 provides details pertaining to the separation (see Section 5 of [43]).

Discussion: In addition to the physical separation between cloud-based services (as explained in Policy Statement 4) comprised of different level data, virtual/logical separation must be configured to add another layer of protection for SAF cloud-based services. This additional layer of protection is to guard against connectivity into one network, from other cloud users sharing the same cloud infrastructure. For example, in the CLASSNET, applications that are solely used by DSTA alone, should have their cloud resources virtually/logically configured so as to prevent other community, such as the SAF, users from accessing them.

8. Policy Statement 6

Statement: SAF personnel must be appropriately cleared before being authorized and enabled to access an associated cloud-based service.

Reference(s): DISA SRG (Section 5.6 of [43]) and Table 7 explain the personnel requirement for each type of cloud-based service, based on the level of information the particular service stores or processes.

Discussion: SAF personnel with appropriate clearance should be authorized to access the associated cloud-based services that host the corresponding (or lower) level of information. In the context of the SAF, a person with military CAT 1 status will be authorized to access cloud-based services comprised of information up to secret

classification; whereas a newly hired recruit, who does not have any clearance, should not be allowed access to any cloud-based services above the level of "public."

9. Policy Statement 7

Statement: SAF cloud users must abide by both national and military laws in affect in Singapore.

Reference(s): SAF personnel must abide by both the national and military laws when using cloud-based services. Under the nation's Personal Data Protection Act, SAF cloud users have to abide by the rules governing the "collection, use, disclosure and care of personal data" [16]. Military law pertaining to the use of SAF IT systems is explained in the discussion paragraph that follows.

Discussion: The current SAF military IT-related laws should also be applied to cloud-based computing. For example, only SAF *authorized* removable storage devices are allowed to be used for the transfer of data from one cloud-based service to another. The authorized storage devices are configured (via encryption) to allow equally or less sensitive data be transferred into cloud-based services comprised of higher level of data, but not the other way round. This helps to prevent any accidental transfer (also known as a leakage) of a higher sensitive data into cloud-based services not configured to protect that level of information. By using SAF controlled storage devices, it can also help to mitigate cyber-attacks executed via unknown/malware-infected removable storage devices (see Section V-D). Another military law example states that only personnel who attend and pass an "IT-awareness course" will be authorized access to cloud-based services. Such adherence to applicable Singapore laws would help to cultivate a safe cloud-based computing environment for the SAF.

10. Policy Statement 8

Statement: The SAF should have a single private cloud for all its branches (i.e., army, navy and air force).

Reference(s): The SAF should leverage a single private cloud to reap the considerable benefits it provides [7].

Discussion: Army, navy and air force branches may their own branch-related systems and different standard operating procedures. The features existing in their current systems may be identical or very similar. For example, features allowing gathering of intelligence and generating the current situation picture (see "recommended cloud features of a military force," in Section VI-B for all other similar features) would be present in all branches' system. Thus, a single SAF private cloud could be configured to provide such baseline features to all its branches, however, with options of adding tailored, branch-specific features configured with virtual/logical separation (see policy statement 5). Moreover, a single SAF private cloud with its IT resources consolidated in a single location would ease the logistics of support and maintenance, as compared to managing three individual "clouds." In the current context, a single SAF private cloud allowing information to be shared across different branches can also help to facilitate unconventional warfare and joint operations where communications is required between all three branches.

F. SUMMARY

In this chapter, by integrating the concept of the OODA loop model and the characteristics of effective C2, we presented various cloud features/services deemed important for the SAF to run its operations in a cloud-based environment. In addition: 1) a decision framework for cloud adoption, 2) a secure cloud-based framework, and 3) a list of seven high-level policy statements were presented in order to aid the SAF in its migration to cloud-based computing. Chapter VII examines the lessons learned during the research, future research areas, and a summary of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION AND FUTURE WORK

A. CONCLUSION

In earlier chapters, cloud computing was shown to increase cost-effectiveness and yield considerable benefits to the healthcare, business and defense sectors. A decision framework for cloud adoption, secure cloud-based framework/guidelines, and recommended policies were then presented to aid the SAF's adoption of cloud-based computing. This chapter concludes this thesis by providing a short summary, lessons learned during the research process, and some possible future research areas.

With technology improving rapidly over the years, many public entities (e.g., healthcare, business, etc.) have adopted cloud-based computing manage their information and information-related operations, mainly in an effort to reduce their overall IT support and management cost. However, it was not immediately clear how this could, or should, be done for the Singapore defense sector. The defense sector handles highly sensitive data and operates differently from typical public sector organizations. As a result, a military may require different cloud features and migration framework to aid its migration into the cloud environment.

From a military perspective, this thesis discussed cloud-computing in general, addressed issues of concern, and provided references to allow further research to be carried out in finding a sound "solution" for the SAF. This research also examined how secure and successful cloud computing has been implemented in public sectors, such as healthcare and business. Then, using the U.S. DOD as an example, this research identified possible areas where the SAF could use cloud computing in support of its operations. The thesis also addressed the issues of incompatible communication devices and systems between participating countries in country-level joint operation (e.g. HADR, etc.). Participating countries could leverage cloud-based services as a common platform for communications, planning and collaboration in a more effective manner.

This thesis culminated, in Chapter VI, with a list of recommended policy statements that the SAF should consider for guidance as it migrates to greater adoption of

cloud-based computing in support of its operations. These policy statements encompass the various aspects of information security (i.e., CIA-triad) deemed most important to the SAF's adoption of a cloud-based computing environment.

1. Lessons Learned

The use of cloud-based services may be significantly less expensive as compared to the use of applications running in traditional IT systems. Various benefits, including scalability, quick deployment, and cost-effectiveness, have been highlighted and explained. As a staff in the SAF, I learned that it may be considerably cost effective (in terms of manpower and cost) for SAF to adopt cloud-based computing for its operations. Having said so, the adoption or movement into cloud services should be done just like the implementation of any other military project; that is with a planned schedule and with calculated risks taken into account.

a. Extensive Cloud Computing Research and Case Studies as Reference

The adoption of cloud-based computing would represent a new operational paradigm for the SAF. As a result, there is some reluctance for the SAF to adopt cloud computing, owing in large part to the myriad unknowns regarding exactly what additional, perhaps unseen, risks it may expose the SAF IT operations to. However, there exist many real life examples in the public sector of other organizations that have successfully migrated, in whole or in part, to which the SAF can look for lessons-learned. The SAF also has access to comprehensive research conducted by NIST and CSCC on cloud computing. Although their examples and research were not cast into a military context, they can still be used as good case studies for the SAF, as the underlining cloud technology is similar.

b. Manpower Savings for the SAF

The support and maintenance of traditional systems located at different premises requires more IT personnel as compared to cloud computing. This is because the cloud-based paradigm allows for more (if not all) IT resources to be consolidated in a single location, thus easing the logistics of support and maintenance. The number of IT

personnel (i.e., signalers) "saved" from the overall conscripted national service soldiers, could also translate into more ground/fighting soldiers, as a percentage of the total the SAF fighting force.

B. FUTURE RESEARCH

1. Organization Structure of the SAF "Cloud" Office

When the SAF adopts cloud-based computing in its operations, a "cloud" office with sufficient staff to handle workloads, such as administration, server configurations, end-station installation, and more, would be necessary. Using cloud-based computing, manpower savings (i.e., signalers from all branches) in the SAF can be used staff this "cloud" office. A study into the staffing and organization of this "cloud" office, scaled as appropriate to serve the needs of the SAF, could be done to aid the SAF adoption of cloud-based computing. In addition, this study should also provide useful staffing information regarding the reduced number of signalers required in each ground unit after cloud-based computing has been implemented.

2. Implementation Study of Military Cloud Features

Chapter VI addressed the various basic cloud features necessary for a military to function and execute its mission. The features identified may work particularly well in a traditional system, because communication with the servers is done via a local area wired network with high (i.e., gigabit speed) bandwidth availability. However, an over-the-air (wireless) link to connect remote cloud-based services and clients/users would yield significantly less bandwidth. This may result in poor service delivery for the users. As such, the SAF would benefit from a study that investigates how the military cloud features could be made to be as reliable as the existing SAF communications infrastructure. This could be done by either, if not both, a) determining how these features could be implemented so as to require less bandwidth, or b) modifying the SAF rules/regulations regarding issues of bandwidth consumption (e.g., email attachments cannot be larger than 20KB in size) in order to counter any reduction in actual operational bandwidth resulting from the cloud-based infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] A. Huth and J. Cebula. (n.d.). The basics of cloud computing [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf. Accessed May 5, 2016.

[2] R. Craig et al. (2009 Nov.). Cloud computing in the public sector. Cisco. San Jose, CA. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/sp/Cloud_Computing.pdf. Accessed Aug. 31, 2016.

[3] What is cloud computing? (n.d.). IBM. [Online]. Available: https://www.ibm.com/cloud-computing/what-is-cloud-computing. Accessed Aug. 31, 2016.

[4] Introduction to cloud computing. (n.d.). Office of the Privacy Commissioner of Canada. [Online]. Available: https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf. Accessed Aug. 31, 2016.

[5] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST, Gaithersburg, MD, Spec. Publ. 800–145, Sep. 2011 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Accessed Sep. 7, 2016.

[6] Statista: The Statistics Portal. Public cloud market vendor revenue worldwide from 2012 to 2026 (in billion U.S. dollars). [Online]. Available: http://www.statista.com/statistics/477702/public-cloud-vendor-revenue-forecast/. Accessed Aug. 31, 2016.

[7] A. Apostu et al., "Study on advantages and disadvantages of cloud computing – the advantages of telemetry applications in the cloud," in *Recent Advances inApplied Computer Science &Digital Services*, 2013, 118–123. [Online]. Available: http://www.wseas.us/e-library/conferences/2013/Morioka/DSAC/DSAC-16.pdf. Accessed Sep. 1, 2016.

[8] O. E. Akkad. (2011, Nov. 11). Outsource IT headaches to the cloud [Online]. Available: http://www.theglobeandmail.com/report-on-business/small-business/sb-managing/outsource-it-headaches-to-the-cloud/article1318511/. Accessed Aug. 31, 2016.

[9] View job vacancies. (n.d.). Defence Executive Office, Singapore. [Online]. Available: http://www.mindef.gov.sg/dxo/careers-details.html#/tab1. Accessed Aug.31, 2016.

[10] M. R. Stytz and S. B. Banks. (n.d.). Identifying and addressing issues in coalition network centric operations using distributed simulation [Online]. Available: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/039.pdf. Accessed Aug. 31, 2016.

[11] Coalition operations demand technology solutions. (2005, Jan.). Armed Forces Communications & Electronics Association. [Online]. Available: http://www.afcea.org/content/?q=coalition-operations-demand-technology-solutions. Accessed Aug. 31, 2016.

[12] Cloud computing. (n.d.).Infocomm Development Authority of Singapore. [Online]. Available: https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/CloudComputing.pdf. Accessed Aug. 31, 2016.

[13] Impact of cloud computing on healthcare (2012, Nov.). Cloud Standards Customer Council. [Online]. Available: http://www.cloud-council.org/deliverables/CSCC-Impact-of-Cloud-Computing-on-Healthcare.pdf. Accessed Aug. 31, 2016.

[14] Benefits of cloud computing. (n.d.). Queensland Government. [Online]. Available: https://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business/cloud-computing-benefits. Accessed Aug. 31, 2016.

[15] C. Coles. (2016, Feb. 16). 9 cloud computing security risks every company faces [Online]. Available: https://www.skyhighnetworks.com/cloud-security-blog/9-cloud-computing-security-risks-every-company-faces/. Accessed Aug. 31, 2016.

[16] Legislation and guidelines. (n.d.). Personal Data Protection Commission, Singapore. [Online]. Available: https://www.pdpc.gov.sg/legislation-and-guidelines. Accessed Aug. 31, 2016.

[17] G. Wallace. (2013, Dec. 23). Target credit card hack: What you need to know [Online]. Available: http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/. Accessed Aug. 31, 2016.

[18] HITECH Act enforcement interim final rule. (n.d.). U.S. Department of Health & Human Services. [Online]. Available: http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html. Accessed Aug 31, 2016.

[19] The defense sector will switch to cloud computing, nevertheless (2014, May 19). Israel Defense. [Online]. Available: http://www.israeldefense.co.il/en/content/defense-sector-will-switch-cloud-computing-nevertheless. Accessed Aug. 31, 2016.

[20] E. Messmer. (2010, Sep. 24). U.S. military takes cloud computing to Afghanistan [Online]. Available: http://www.computerworld.com.sg/resource/cloud-computing/us-military-takes-cloud-computing-to-afghanistan/?page=3. Accessed Aug. 31, 2016.

[21] V. Kundra. (2010, May 20). State of public sector cloud computing [Online]. Available: https://cio.gov/wp-content/uploads/downloads/2012/09/StateOfCloudComputingReport-FINAL.pdf. Accessed Aug. 31, 2016.

[22] A new paradigm in cloud computing (2013, May). Infocomm Development Authority of Singapore. [Online]. Available: https://www.ida.gov.sg/~/media/Files/About%20Us/Newsroom/Speeches/2013/1505_CloudAsia2013/CloudComputingFactSheet.pdf. Accessed Aug. 31, 2016.

[23] Defence Science and Technology Agency of Singapore. (2016). DSTA horizons. DSTA. Singapore. [Online]. Available: https://www.dsta.gov.sg/docs/dsta-horizons-2016/download-full-pdf.pdf?sfvrsn=0. Accessed Aug. 31, 2016.

[24] Fundamental security concepts. (n.d.). Cryptome. [Online]. Available: http://cryptome.org/2013/09/infosecurity-cert.pdf. Accessed Aug. 31, 2016.

[25] Confidentiality, integrity, and availability (CIA triad). (n.d.). TechTarget. [Online]. Available: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. Accessed Aug. 31, 2016.

[26] Top threats to cloud computing v1.0 (2010, Mar.). Cloud Security Alliance. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. Accessed Aug. 31, 2016.

[27] C. Barron et al. "Cloud computing security case studies and research," in *Proceedings of the World Congress on Engineering*, London, UK, 2013, vol. 2, pp. 1287–1291.

[28] J. Rutkowska. (2006, Jun. 22). Introducing Blue Pill [Online]. Available: http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html. Accessed Aug. 31, 2016.

[29] K. Kortchinsky. (2009, Jun. 29). Cloudburst [Online]. Available: https://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf. Accessed Aug. 31, 2016.

[30] M. Osterman and M. Delima. (2016, Aug. 4). Briefings part 3: Secure in the cloud —securing email migration to Office 365 [Online]. Available: https://www.isc2.org/security-briefings/default.aspx?commid=212381. Accessed Sep. 1, 2016.

[31] M. Prince. (2012, Jun. 4) The four critical security flaws that resulted in last friday's hack [Online]. Available: https://blog.cloudflare.com/the-four-critical-security-flaws-that-resulte/. Accessed Sep. 1, 2016.

[32] Social engineering. (n.d.). TechTarget. [Online]. Available: http://searchsecurity.techtarget.com/definition/social-engineering. Accessed Sep. 7, 2016.

[33] What your business should know about social engineering. (2013, Oct. 21). GAA Accounting. [Online]. Available: http://www.gaaaccounting.com/what-your-business-should-know-about-social-engineering/. Accessed Sep. 7, 2016.

[34] Stuxnet. (n.d.). *Wikipedia*. [Online]. Available: https://en.wikipedia.org/wiki/Stuxnet. Accessed Sep. 1, 2016.

[35] D. Lee. (2012, May 28). Flame: Massive cyber-attack discovered, researchers say. *BBC News* [Online]. Available: http://www.bbc.com/news/technology-18238326. Accessed Sep. 7, 2016.

[36] OODA loop. (n.d.), *Wikipedia*. [Online]. Available: https://en.wikipedia.org/wiki/OODA_loop. Accessed Sep. 1, 2016.

[37] J. Boyd. (n.d.). Summary of OODA model by Boyd. [Online]. Available: http://www.valuebasedmanagement.net/methods_boyd_ooda_loop.html. Accessed Sep. 1, 2016.

[38] B. Brehmer, "The dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control," presented at the 10th International Command and Control Research and Technology Symposium, 2005. [Online]. Available: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf. Accessed Sep. 1, 2016.

[39] V. Creveld, "Introduction: On command," in *Command in War*, Cambridge: Harvard University Press, 1985, p. 7.

[40] R. R. Leonhard et al. (2010). A concept for command and control. *Johns Hopkins APL Tech. Dig*. [Online]. *29*(2). pp. 157–170. Available: http://www.jhuapl.edu/techdigest/TD/td2902/Leonhard.pdf. Accessed Sep. 1, 2016.

[41] Migrating applications to public cloud services. (2013, Dec.). Cloud Standards Customers Council. [Online]. Available: http://www.cloud-council.org/deliverables/CSCC-Migrating-Applications-to-Public-Cloud-Services-Roadmap-for-Success.pdf. Accessed Sep. 7, 2016.

[42] Security for cloud computing: Ten steps to ensure success. (2015, May). Cloud Standards Cuntomer Council. [Online]. Available: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf. Accessed Sep. 1, 2016.

[43] Cloud computing security requirement guide. (2016, Mar). Defense Information Systems Agency. [Online]. Available: http://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r2.pdf. Accessed Sep. 7, 2016.

[44] M. Vickers. (2016, Sep). "DOD information security program: marking of classified information," Defense Information Systems Agency. [Online]. Available: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf. Accessed Sep. 8, 2016.

[45] James Cook, (2014, Oct). "The U.S. Government Is Going To Store Top Secret Documents In The Cloud," Business Insider. [Online]. Available: http://www.businessinsider.com/the-us-government-is-going-to-store-top-secret-documents-in-the-cloud-2014-10. Accessed Sep. 15, 2016.

[46] National Institute of Standards and Technology. (2015, Jan). Security and privacy controls for federal information systems and organizations. NIST. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Accessed Sep. 9, 2016.

[47] National Institute of Standards and Technology. (2015, Dec). FedRAMP security assessment framework. DOD. [Online]. Available: https://www.fedramp.gov/files/2015/01/FedRAMP-Security-Assessment-Framework-v2-1.pdf. Accessed Sep. 9, 2016.

[48] National Institute of Standards and Technology et al. (2014, Jun). Security Assessment Plan (SAP) Template. DOD. [Online]. Available: https://www.fedramp.gov/resources/templates-2016/#. Accessed Sep. 9, 2016.

.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California