Volume 1 No. 3, July 2011 ISSN-2223-4985
International Journal of Information and Communication Technology Research

http://www.esjournals.org

A Roadmap for Transitioning an Information Assurance Program and Others to Cloud Computing

Samir Tout
Eastern Michigan University, Ypsilanti, MI, USA

ABSTRACT

Cloud computing (CC) has gained a lot of popularity in the past few years. Since we published a paper about CC in ISECON'2009, several new developments have taken place, including new standards by the National Institute of Standards and Technology (NIST) and other relevant research. This paper explores such recent standards and research, and cites some of the challenges facing organizations that are contemplating to move from traditional in-house infrastructure to the cloud. The paper subsequently delves into an evaluation of the potential for that transition at Eastern Michigan University's Information Assurance (EMU-IA) program. It follows a process of assessing the requirements for typical exercises from key courses and how these can benefit from cloud computing. The paper then presents some recommendations for the deployment model, based on a weighted factor analysis, as well as general recommendations in an effort to establish a preliminary roadmap to pursue this transition further in the future.

Keywords: *Cloud Computing, Higher Education, Information Assurance, Security, Software as a Service (SaaS)*

1. INTRODUCTION

Cloud Computing (CC) is a relatively modern technology that has gained considerable attention in the past few years. Partly based on the outdated Application Service Provider (ASP) that met its demise in the 1990's, CC has taken advantage of the larger leaps in technological advancements that were achieved lately and has therefore revolutionized the way businesses implement their IT services by providing options that were otherwise not feasible during ASP times.

One of the key tenets of CC entails reducing in-house data centers and delegating either part of or the entire Information Technology (IT) infrastructure to a third party. This has several advantages such as reduced maintenance costs and the ability to focus on strategic goals. However, CC also comes with some lurking disadvantages that have kept some companies from making such a leap of faith into this new realm. In [1], we outlined some of the preliminary concepts related to CC along with key benefits and limitations that face its adopters, notably in institutions of higher education. This paper builds on that work, reflects on some of our projections therein, and expands on them to include current trends, research and standards that have emerged in the past two years. We also evaluate the benefits and challenges of adopting CC for our Information Assurance program and outline a preliminary roadmap for achieving that goal. We extend this further to provide a list of recommendations for EMU as well as higher education institutions when adopting this prolific technology.

The rest of this paper is organized as follows: Section 2 cites recent research and standards that have evolved regarding this topic. Section 3 evaluates the potential for CC adoption at EMU by inspecting computing requirements for key courses in various IA degrees. Section 4 provides recommendations for one or more deployment models, based on a weighted factor analysis that utilizes the NIST standards in [10]. This section also provides general recommendations that serve as a preliminary plan for future adoption of CC. Section 5 contains the conclusion.

2. RECENT DEVELOPMENTS IN CLOUD COMPUTING

2.1 Relevant Research

Considerable developments have taken place in the realm of cloud computing since we published our paper in 2009 [1]. One such key development is SP 800-145 by NIST, which uses industry-standard terms to provide a concise description of Cloud Computing based on five characteristics, three service models, and four deployment models [2]. This will be explored further in next section.

Also, recently, one of our esteemed colleagues at EMU, Professor Stevan Mrdalj, published a paper titled "Would Cloud Computing Revolutionize Teaching Business Intelligence Courses?" [3] In it, he explored the potential for leveraging cloud computing to teach Business Intelligence courses by presenting their computing requirements in a standalone version, a local area network based version, and a web-enabled version. He subsequently drew a comparison between those and a cloud-based counterpart and their perceived difficulties then concluded that "cloud computing is an attractive solution for business schools wanting to implement cost-effective, rapid and dynamic environments for their BI courses."

Furthermore, Quest Software commissioned a recent study [4] by Norwich University's School of Graduate and Continuing studies in which they surveyed government and higher education personnel that are mostly in a management or executive role. The objective

was to "gauge perceptions of virtualization and cloud computing among government and higher education IT management professionals." The study indicated that a large percentage of those polled stated that a hybrid cloud model would best meet their immediate needs followed by a private cloud. The study also indicated that roughly 36% of respondents from higher education stated that cost saving is the major driver for moving to the cloud and that roughly 61% see benefits from establishing a national cloud that is dedicated to higher education. Also, roughly 63% of those surveyed from higher education indicated a positive and optimistic attitude toward cloud computing. Finally, approximately 40% indicated that the biggest barrier to the adoption of a public cloud is the vulnerability to security breaches while 11% stated the same about a private cloud.

Another relatively recent research by the EDUCAUSE Center for Applied Research (ECAR) explored – through an online survey of IT leaders – the benefits, challenges and complexities surrounding cloud computing as well as other alternative sourcing strategies [5]. Their summary of findings provides an insight into the plans of key market players in terms of adopting outsourcing and specifically cloud-computing. For instance, 84% of institutions reported some use of alternative IT sourcing, which is a significant number. However, one interesting finding that relates to our IA program reports that "the least frequent use of alternative sourcing is for areas related to information security", which as they state in their results, scores a meager 4.5%. Furthermore, 50% of respondents stated that they employ some form of SaaS versus other deployment models. The good news is that the majority of respondents to that survey stated that they expect incremental growth in adopting various alternative sourcing, including Cloud Computing. This research comes up with three main recommendations in order to help institutions better plan for the adoption of cloud computing: Engaging IT governance to guide the transition to the cloud, upgrading IT organization members' competencies to match the new demands of cloud computing such as technology integration and contract negotiations, and finally establishing a prioritized list of candidates to transition to the cloud (business continuity/disaster recovery, virtual labs, computing cycles, data storage, e-mail, etc.)

Even the U.S. federal government decided to jump on the cloud computing wagon and recently introduced apps.gov [6], which provides Infrastructure-as-a-Service (IaaS) offerings to federal, state, local, and tribal governments.

Furthermore, other individual efforts have been initiated to encourage the use of cloud computing. For instance, in a blog post at InfoWorld, William Hurley wrote a letter to President Barack Obama, asking him to push for the creation of a cloud-computing platform for higher education [7].

Moreover, [8] reports on the use of cloud-based file organization tools, such as Dropbox, SugarSync, and others that allow students to share their work and readily synchronize them among various platforms and devices. While raising some concerns of privacy and security, this provides value to students, as they would overcome the limitations of manually having to copy their files from one device to another. Although simple in nature, such tools would be an attractive proposition to students, as they would constitute a convenient technology that helps them become more efficient.

2.2 Standards

Several new standards have emerged in past two years since we published [1]. This section will focus on those produced by NIST due to its leading role in establishing standards at the national level and its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002.

In January 2011, NIST produced a draft of Special Publication (SP) 800-145 titled "The NIST Definition of Cloud Computing" with the purpose to "enhance and inform the public debate on cloud computing" [9]. In it, NIST defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST also divided it into five essential characteristics, three service models, and four deployment models. In these definitions and in the rest of this document, the terms *subscriber*, *consumer*, and *client* will be used synonymously to refer to the party that consumes the cloud services and resources while *cloud provider* and *cloud supplier* will refer to the party that supplies such services and resources. Several of these definitions will be leveraged in our analysis later in this paper.

As per [9], the five CC characteristics are:

1. **On-demand self-service:** This allows subscribers to provision computing resources (such as storage, memory, processing, network bandwidth, etc.) readily with little interaction with cloud providers.
2. **Broad network access:** All cloud resources are available over the network (mostly the Internet), thus allowing interaction with a variety of heterogeneous devices.
3. **Resource pooling:** This focuses on the concept of multi-tenancy, which allows the demands of subscribers to govern the dynamic allocation of resources and promotes location independence.
4. **Rapid elasticity:** This allows the speedy and automatic allocation/de-allocation of resources and thus promotes scalability with the notion of unlimited availability to the consumer.
5. **Measured service:** This refers to the pay-per-use business model by enabling the metering of

resource usage, thus promoting transparency between the subscriber and the provider.

As per [9], the three service models are:

1. **Software as a Service (SaaS):**
   In this model, subscribers use a thin client, typically a Web browser to access applications running on the provider's infrastructure, with no control over that infrastructure.
2. **Platform as a Service (PaaS):**
   The provider makes available to the subscriber a set of tools that allow them to create and deploy applications onto the provider's cloud infrastructure. The subscriber has no control over that infrastructure but some over the hosting environment.
3. **Infrastructure as a Service (IaaS):**
   The provider makes available to the subscriber key infrastructure resources with some control over the operating system, applications, and sometimes networking components such as firewalls, routers, etc.

As per [9], the four deployment models are:

1. **Private cloud:**
   A cloud infrastructure is dedicated to an organization on/off its premises and either managed by it or delegated to another organization.
2. **Community cloud:**
   A cloud infrastructure that is shared by more than one organization one/off their premises and either managed by it or delegated to another organization.
3. **Public cloud:**
   A cloud infrastructure is typically open to the general public.
4. **Hybrid cloud:**
   A cloud infrastructure is composed of more than one cloud of any of the three above types, bound together by standard/proprietary technology.

In May 2011, NIST produced a draft of SP 800-146 titled "Cloud Computing Synopsis and Recommendations" with the purpose to "provide recommendations for information technology decision makers, and to explain the cloud computing technology area in plain terms" [10]. After going through this document, it became evident how valuable it is in guiding the efforts of organizations, such as ours, that plan to transition to the cloud. Meanwhile, it demonstrates that this is still a young field with a lot more to explore until it reaches a stable level of maturity. Some of the key pertinent highlights from this standard include the detailed discussion of different deployment models and their implications. Please refer to the later section titled "EMU-IA Plans and Recommendations" for further details.

2.3 Challenges

There is no doubt that higher education has unique needs that must be accommodated. For instance, in terms of compliance, educational institutions are required to safeguard student information, per the Family Educational Rights and Privacy Act of 1974 (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). University professors are faced with the challenge of how to apply such requirements with the constantly evolving technologies that are used to store student records, including cloud-based storage. Three strategies were suggested in [11] to handle such challenges: employ policies or consent forms to regulate the compliance of learning, implement local instances of cloud-based tools to ensure the protection of student privacy, and engaging students and faculty in the dialogue about the importance of privacy.

Furthermore, higher education institutions were the incubators to several ubiquitous current-day technologies. For instance, among other innovations, UCLA, Stanford, UC Santa Barbara, and University of Utah housed the first four nodes of the Internet's parent network, Arpanet. However, universities are typically late adopters, mostly due unique policies that govern the processing, storage and dissemination of higher education related information, security concerns, and unclear cost structure [12]. This may potentially place additional hurdles in the way to adopt cloud computing.

Universities also place a special attention to public trust since they are considered to be the students' *in loco parentis* and the custodians of sensitive and sometimes personal information of human subjects that are involved in research studies. Therefore, it is expected that the approval of such a shift in hosting and processing this information to a third party would face some resistance.

3. CLOUD COMPUTING POTENTIAL AT EMU-IA

The following sections provide some analysis pertaining to the use of Cloud Computing at our Information Assurance program at EMU (EMU-IA). It is hoped to be the initial point for establishing a process to evaluate the readiness to make such a move.

3.1 The EMU-IA degrees

It is a known fact that technologies are continuously and expeditiously evolving at a pace that is hard to match. This puts more pressure on institutions of higher education, notably those that are specialized in the field of technology; case in point is the EMU College of Technology (CoT) that houses two schools: the School of Technology Studies (STS), under which falls our Information Assurance program, and its sister School of Engineering Technology (SET). The IA program has an undergraduate degree, a graduate degree, and a Ph.D. in

Technology with an IA concentration. This section elaborates on some of the key offerings in each of these degrees and explores a possible plan for transitioning them, completely or partially, to the cloud.

3.1.1 Undergraduate IA Curriculum

The undergraduate IA degree is composed of a set of foundation courses along with three main tracks: Information Assurance Management, Applied Information Assurance, and Information Assurance Encryption [13].

The foundation group contains Computer Science, Math, and IA courses. One of the key IA courses is IA 103 "Information Security Overview" which, as per its name, introduces students to the basics in Information Security: its definition, history, security systems development life cycle, the need for security and various threats/attacks, the legal/ethical laws surrounding IA, risk analysis (including weighted factor analysis and cost-benefit analysis), policy development, firewall configuration/rule tables, intrusion detection/protection (both host-based and network-based flavors).

The IA Management track contains more focus on the organizational and administrative aspects of IA, such as IA 329 "Policy Development in Information Security", IA 425 "Project Management", and IA 422 "End-User Systems." The latter is considered to be a representative course in this track. It delves into the systems analysis and design aspects of IA, which include feasibility studies, preliminary investigations, Gantt and PERT/CPM charts, estimations, Data-Flow Diagrams, Object-Oriented Analysis, and I/O Design.

The Applied IA track focuses on IA applications that have a practical aspect in the real life. Key courses in this track include IA 325 "Cyber Crime Investigation I" and IA 327 "Computer Forensics I." The latter is a representative course, which focuses on computer forensics investigations, digital evidence, and investigative software tools.

Finally, the IA Encryption revolves around encryption-related Math courses along with research in IA. One representative course is Math 409 "Cryptography", which covers breaking codes and ciphers, primes, probability, and public key cryptography.

3.1.2 Graduate IA Curriculum

The graduate IA program has three tracks: Information Assurance, Network Security, and Digital Investigations [14]. One key representative course for all these tracks is IA 642 "Enterprise Security" which covers the majority of security domains in the CISSP certification.

3.1.3 Ph.D. IA Curriculum

The Ph.D. in Technology with a concentration in Information Assurance has a minimum of 59 credits, 15 of which are in the IA field while the majority of the rest are related to dissertation research [15]. This study will focus on a sample grant proposal that could benefit from cloud computing.

3.2 Computing Requirements for IA Courses

This section will take a first step toward determining the computing requirements for each of the undergraduate, graduate, and Ph.D degrees and will treat the above-mentioned key courses as their representatives. We will explore their requirements in terms of cloud computing and recommend a good fit for a specific service model, according to the earlier mentioned NIST definitions. As a long-term plan, this process will be applied to the rest of the courses to come up with a consolidated plan for what it takes to transition these offerings to the cloud. It is worth noting that the choice of a deployment model would depend on more than specific exercises or even courses, as it entails assessing the cost, feasibility, and applicability not only to EMU-IA, but also to EMU in general. Therefore, this choice is assumed to follow the recommendation that is established later in that regard.

3.2.1 The Undergraduate IA Curriculum

The IA foundation group:

As mentioned earlier, IA 103 "Information Security Overview" is a key foundation course that covers essential areas in information security. Although it is of introductory nature, this course contains several fundamental exercises that introduce students to important security concepts, in this case: firewall configuration basics. For instance, Fig. 1 depicts a sample network configuration exercise, adopted from [16], which involves setting up proper firewall rules to filter out unwanted traffic. Table 1 is an example of five such rules.

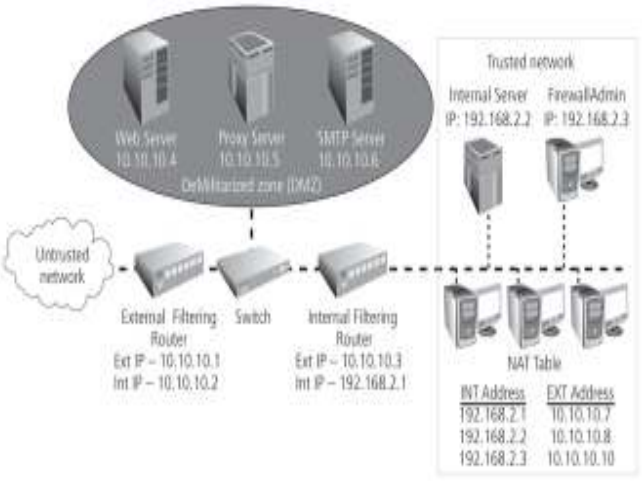

Fig. 1. Sample network configuration [16].

Table 1: Sample filtering rules

Rule #	Source Address	Source Port	Dest. Address	Dest. Port	Action
1	Any	Any	10.10.10.0	>1023	Allow
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny

As shown in Fig. 1, the infrastructure of this specific exercise requires having a Web Server, a Proxy Server and an SMTP Server in a demilitarized zone (DMZ) that is connected through a switch – and separated through an internal filtering router from – a trusted (NAT'ed) network. Furthermore, an external filtering router sits between the switch and an un-trusted external network. Table 1 shows, among others, five possible firewall rules that are established on the external filtering router. Although we had several in-house components that I leveraged while teaching this course in Fall'2009, after running into some limitations related to equipment setup, facility sharing, and cost (which is quite typical in many universities as well as in the industry) it became clear that leveraging a more flexible external facility would be beneficial.

This would be a good fit for an IaaS service model that provisions the above network resources, either physical or virtualized. As per [9], the subscriber (in this case, EMU-IA) would be given control by the cloud vendor over the operating system and the networking components, in this case the firewalls/routers.

The IA Management track:

A representative course is for this track is IA 422 "End-User Systems." The following sample exercise, adopted from [17], exemplifies one of the typical requirements for exercises in this course. In this exercise a team of systems analysts is working on an anti-spam project with the following requirements:

- The Anti-Spam project will cost $45,000 to develop in Year 0. After it is operational, it will have a five-year useful life. Operational costs will be $19,000 per year for Years 1-4 and $45,000 in Year 5.
- Project benefits will be $40,000 in Year 1 and will increase 10% in each of the following years.

Students are expected to apply concepts that they learned in class and create a worksheet that shows costs and benefits for years 0 – 5 and helps them determine the payback period. The following is a typical outcome of this exercise:

Table 2: Payback analysis Exercise

Year	Costs	Cumulative Costs	Benefits	Cumulative Benefits
0	45000	45000		
1	19000	64000	40000	40000
2	19000	83000	44000	84000
3	19000	102000	48400	132400
4	19000	121000	53240	185640
5	45000	166000	58564	244204

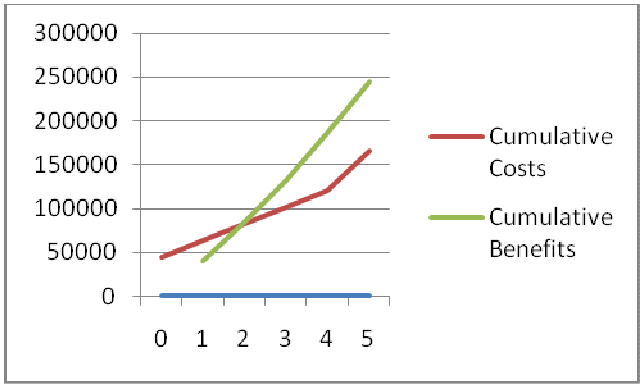

Fig. 2. Line chart showing payback period

This would be a good fit for a SaaS service model that provisions an online spreadsheet application, such as through Google Docs. As per [9], the subscriber (in this case, EMU-IA) would be given access by the cloud vendor to the spreadsheet application running in its cloud infrastructure. However, EMU-IA would not be granted any control over the operating system nor other infrastructure items outside of the application.

The Applied IA track:

As mentioned earlier, IA 327 "Computer Forensics I is a representative course for this track as it focuses on computer forensics investigations, digital evidence, and investigative software tools. The following is a typical exercise that involves the use of Link Logger, a tool that helps monitor firewall/router traffic as part of a network forensics investigation. This is adopted from [18].

"Use Link Logger to monitor network traffic:

- Launch the Link Logger program
- Initiate ping traffic
- Check for scans/attacks coming from a specific source IP.
- Assess if these constitute a threat to the network."

Other similar forensics exercises involve the use of EnCase, a forensic software suite that includes tools to

support various forensics investigations. This would fit with the model of SaaS whereby a VM would be provisioned by the provider and put at the subscriber's disposal, with Link Logger, EnCase, or even other similar tools installed on it, such as Computer Online Forensic Evidence Extractor (COFEE) [19]. Of course there are some security concerns regarding this setup, if it were to be used for real life forensic investigation scenarios, especially with EnCase and COFEE. This is mostly due to the sensitive nature of data that are typically involved therein. However, considering that data in such exercises are typically either obfuscated or canned, this concern is mitigated.

As to the IA Encryption track, it will be combined with the next section regarding the IA Graduate Degree, specifically when we give an example of an exercise for IA 642 "Enterprise Security" which covers the encryption domain in the CISSP certification.

3.2.2. The Graduate IA Curriculum

IA 642 "Enterprise Security":

This course is a good representative for the Information Assurance and Network Security tracks in the IA graduate curriculum. It covers the majority of security domains in the CISSP certification. The following exercise demonstrates how to solve a problem under the Encryption Domain. It is adopted from [20]

"In this project, you send and receive encrypted e-mail messages. Required for this project: Windows 2000, XP, or Vista and Administrative access to the Windows OS for purposes of installing software.

1. Obtain a copy of GnuPG (GPG) from http://ww.gnupg.org and install it on your system.
2. Find another person who will do the same on their system, so that you can exchange messages. Create a private-public key pair.
3. Send your public key to the other person. Have the other person send their public key to you.
4. Import the other person's public key using the Keys>Import command.
5. Using your local e-mail program (Outlook, etc.) create an encrypted e-mail message. Alternately, encrypt a file using the other party's public key. Have the other person encrypt a file or message with your public key. Send the encrypted files/messages to each other.
6. Open the message/file sent from the other person. What are your observations?
7. If available, have a third person encrypt a file with their public key and send to you. Try to open the file. What are your observations?"

This would fit with the model of PaaS whereby a VM would be provisioned by the provider and put at the subscriber's disposal, with Public Key Infrastructure (PKI).

3.2.2. The Ph.D. IA Curriculum

As part of research conducted in our Ph.D. in Technology program, in the IA concentration, a grant proposal involved the using a game-based approach to train high school students on key defensive techniques by using an Intrusion Detection System (IDS), such as Snort [21] along with a virtual honeypot. The idea was to divide students into two teams of *attackers* (simulated hackers) versus *defenders*, whereby the latter team would lure the hackers to attack a local server that poses as a legitimate server with tantalizing and valuable data.

Below is the architecture diagram that provides the details of the planned Honeypot design.

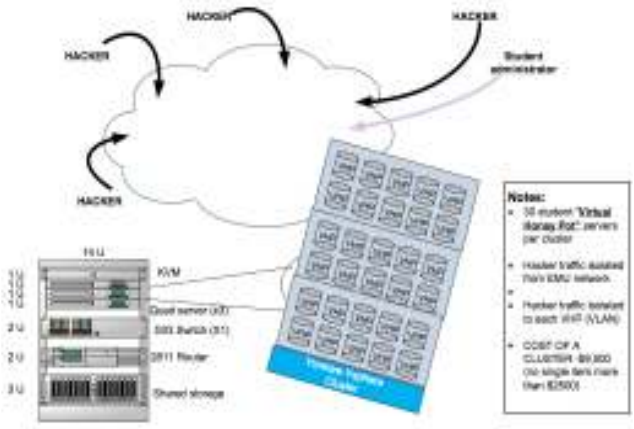

Fig 3 Architecture Diagram for Honeypot Hosting

As shown above, this would be a good fit for an IaaS model, whereby the cloud provider would place the above resources at the disposal of EMU-IA, while giving students adequate access privileges for the administration of the various involved components. At the time of the proposal, the estimated cost of this setup, if it were pursued in-house, was around $30,000. The savings that would be achieved by moving this to the cloud remain to be fully determined, as it would be important to assess the usage demands through a pilot phase. However, the gain is expected to be considerable since the exercises would take place at a specific time with a pre-determined attack-defense scenario that would lower the usage of the cloud resources or at least limit it.

4. EMU-IA RECOMMENDATIONS

This section provides recommendations in terms of a specific deployment model as well as general recommendations for pursuing the transition to cloud computing.

4.1 Recommendation for the Deployment Model

In [10], the authors established scopes for the various deployment models mentioned earlier. These include: the general scope that applies to all deployment models, the on-site-private scope that applies to private clouds at the subscriber's premises, the outsourced-private that applies to private clouds with the server resources outsourced to a third-party, the onsite-community that applies to community clouds on the subscriber premises, outsourced-community where community clouds are hosted on a third party, and finally the public scope applies to the public clouds. They subsequently used these scopes to describe various cloud scenarios into more detailed statements, such as network dependency, IT skills, workload locations, risks from multi-tenancy, and data import/export and performance limitations and they recommended that organizations contemplating the use of cloud computing consider these statements (which we also refer to in this document as "effects").

Weighted Factor Analysis:

In an effort to quantify the advantages of the earlier mentioned scenarios, this paper conducts a weighted factor analysis that is based on the content of NIST's SP 800-146 in [10]. These details are summarized in Table 3 in Appendix A. This table was augmented with additional information in order for us to conduct the weighted factor analysis. For instance, a weight (shown in parentheses in the table) has been assigned to each of the effects with the following interpretations. Note that the weights are assigned based on an initial assessment in the context of EMU-IA and these may be adjusted when applied to other contexts and as further dialogue takes place with other organizations, as stated later.

- *Network dependency* was given a score of (2) since that is an important factor. However, since connectivity is generally available, the score was not raised to 3.
- *Subscribers' need for IT skills* was given a score of (1) since in the College of Technology, we expect to have enough IT skills to handle at least the preliminary phases of this transition.
- *Workload locations* is not a very crucial effect and therefore was given a score of (1)
- *Risks from multi-tenancy* was given a score of (1) because it is not very crucial to pin our workload to a specific location.
- *Data import/export and performance* was assigned a weight of (1) since, except for capacity tests, the majority of our exercises do not require high performance or demanding imports/exports.
- Since cost is a major driver, the effect of *Up-front migration costs* was given a weight of (3).
- *Resources available* was given a score of (2) since it is typically important to ensure that student exercises are not delayed extensively due to the lack of resources.

Furthermore, an additional "Picks" column was added to show our selection for every effect, based on our situation at EMU-IA with the following interpretations. Note that the picks were made based on the context of EMU-IA and these may be adjusted when applied to other contexts.

- For *Network dependency*, we picked OPC and PC since OPC provides limited dependency while the Internet, in the case of PC, has been used for more than a decade now for similar endeavors and has proven to be reliable to a certain extent. OSPC, OCC, and OSCC were not chosen since they added additional proprietary resources and involved more than one organization.
- For *Subscribers' needs for IT skills*, OSPC, OSCC, and PC were chosen since, compared to the others, they requirement less additional skill that were restricted to access policies.
- For *Workload locations*, OPC and OSPC were chosen since these two cases are more restricted and therefore provide more subscriber control.
- For *Risks from multi-tenancy*, we selected all but PC due to its higher security and reliability risks (see Table 3)
- For *Data import/export and performance*, we selected all but PC since they are all limited by network capacity, which can be faster leased lines, etc.
- For *Potentially strong security*, we selected OPC and OSPC since they depend on less perimeters to harden than other choices.
- For *Up-front migration costs*, we chose OSP, OSCC, and PC since they have a modest-to-significant cost, versus the others that have a significant-to-high cost, as per [10].
- For *Resources available*, we picked PC since it typically provides maximum elasticity among all choices.

The following scores can subsequently be calculated for each of the scenarios, using the weighted factor method. Please refer to Table 3 in Appendix A for more details.

- Onsite Private Cloud (OPC): 2+1+1+1+1 = 6
- Outsourced Private Cloud (OSPC): 1+1+1+1+1+3 = 8
- Onsite Community Cloud (OCC): 1+1 = 2
- Outsourced Community Cloud (OSCC): 1+1+1+3 = 6
- Public Cloud (PC): 2+1+3+2 = 8

Based on the above analysis, and considering the current state of affairs, with budget cuts and no significant dialogue being initiated regarding CC, our

recommendation is to start with a hybrid model whereby we would transition labs for only a few courses, notably introductory ones, such as IA 103 to a public cloud, while exploring the prospects of an outsourced private cloud. This will mitigate the concerns raised in [11] regarding student privacy whereby labs do not expose students' personal information that is protected by FERPA while providing the ability to utilize ready infrastructure for labs that contain dummy data, such as the ones mentioned earlier. Subsequently, we would start the dialogue with other organizations within and outside of EMU to plan for a community or even a national cloud. This is supported by the earlier mentioned research by Quest in [4], which stated that 61% of those polled from higher education perceived benefits from establishing a national cloud for higher education. Finally, although the above quantitative analysis showed that onsite community cloud scored considerably lower than others, this may change after that dialogue is initiated. Therefore, as outlined in the general recommendations below, it is important to revisit this analysis after engaging other organizations.

4.2 General Recommendations

Despite all the benefits that were outlined earlier in this paper as well as others, we plan to gradually transition to the cloud, mostly based on the earlier recommendations as well as the following ones. Some of these contain a short-term component that focuses on the IA program and a long-term component that attempts to spread the benefit to the whole EMU institution as well as others. The idea is to move to cloud computing in phases, with the IA program being the first phase, thus paving the way for and followed by other programs, departments, schools, colleges, and then ultimately to EMU and other higher education institutions. This is while coordinating with other key players and staying on top of the latest standards and research developments in this regard. One of driving forces behind these recommendations is the positive attitude toward CC in higher education, as stated earlier in the Quest study in [4]. The general recommendations are:

1. Form a group that contains at least two representatives from the IA faculty and two from the administration (short-term) or a representative from every department/school at EMU (long-term). As suggested in [11], also involve student representatives to get their point of view. This group would explore current learning practices and the feasibility and requirements of moving to the cloud while benefiting from work that has already been done in that regard, notably coordinate with Professor Stevan Mrdalj from the EMU business school to exchange lessons-learned and establish a consolidated plan to reduce redundancy.
2. Opening the dialogue with other organizations to shed more light on the weighted factor analysis that was discussed in the previous section and revisit it in light of that dialogue then mature it to become more reliable and conducive to making decisions for transitioning to a suitable cloud model.
3. Create a strategic plan for adopting cloud computing. This plan should start with the short term goals then expand them to longer term ones that establish a concerted effort among various departments and schools at EMU.
4. Since cost is a major player in making the move to the cloud, and due to the latest budget cuts that have curtailed similar projects around the nation, we would like to gain a solid understanding of cost implications of such a move. This is very important especially that these cuts may very well encourage the exploration of alternative sourcing, such as cloud computing. Much like other relatively large universities, EMU has several colleges and many underlying schools and departments. The majority of these manage their own commodity computing services and have therefore established "financial silos" in terms of operating and infrastructure costs that would be essential to understanding the overall cost of that transition. This exerts some pressure on IT organizations to expand their financial analysis capabilities in order to be able to conduct a proper assessment based on their knowledge of the technical services as well as their cost versus that of their cloud substitutes.
5. Another recommendation that is related to financials and applicable to all universities is to start the dialogue with the administration to change the culture of budget allocation to match the on-demand nature of cloud services versus the traditional static allotments that would otherwise become impractical with the dynamic rental demands.
6. Engage a legal team to understand and plan for compliance to laws that ensure students' privacy, such as FERPA. As mentioned in [11], it may be worth it to follow the steps of higher education institutions, such as North Carolina State University whereby they created a FERPA Privacy Checklist that helps guide faculty in various course offerings, including online courses. Also use this legal team to carve out the details of Service Level Agreements (SLAs), policies, and consent forms to protect students as well as the university.
7. Conduct a pilot for the transition to the cloud whereby the above curriculum-to-cloud process of course evaluation is rolled out to other courses in the IA program and share them with other programs in the School of Technology Studies (STS), College of Technology (CoT), other colleges, and ultimately roll them out to EMU and to other willing universities.

5. CONCLUSION

This paper provided some background of current research and standards that have recently evolved in the realm of cloud computing. It also analyzed the requirements of exercises that are conducted in some of

the key courses in the EMU-IA program and provided a recommendation for the proper service models that would fit these requirements. A quantitative analysis was also conducted, based on the standards in [10] and provided a preliminary process to recommend a proper deployment model. Finally, a set of general recommendations were provided in order to pave the way for a roadmap to adopting cloud computing at EMU-IA and subsequently at other parts of EMU. We believe that CC will provide value to the EMU-IA courses and will enhance our offerings and streamline our costs. However, there is a need to do enough due diligence by implementing the above recommendations and following through on that roadmap to ensure we maximize the value of CC to EMU and other higher education institutions.

ACKNOWLEDGMENTS

I would like to thank Dr. William Sverdlik for his insight into some of the latest developments in Computer Science, Prof. Skip Lawver for his oversight of the IA courses and Prof. James Banfield for providing the Architecture Diagram for Honeypot Hosting in Fig. 3 and for providing some of the exercises in IA 103.

REFERENCES

[1] Tout, S, W Sverdlik, and G Lawver (2009). *Cloud Computing and its Security in Higher Education*. In The Proceedings of the Information Systems Education Conference (ISECON) 2009, v 26 (Washington DC): §2314. ISSN: 1542-7382.

[2] Metz, R., (2010). Cloud Computing Explained. Retrieved on 7/18/2011 from http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/CloudComputingExplained/206526.

[3] Mrdalj, S. (2011). Would Cloud Computing Revolutionize Teaching Business Intelligence Courses?" Issues in Informing Science and Information Technology, Volume 8, 2011.

[4] Quest (2011). A Pulse on Virtualization & Cloud Computing. Prepared for Quest Software by Norwich University, School of Graduate and Continuing Studies April 2011.

[5] Goldstein, P. (2009). Alternative IT Sourcing Strategies: From the Campus to the Cloud. EDUCAUSE Center for Applied Research (ECAR).

[6] GSA. Apps.gov. Retrieved on 7/11/2011 from https://www.apps.gov/cloud/main/start_page.do

[7] Hurley, W. (2009). Higher education needs a national computing cloud. Retrieved on 7/15/2011 from http://weblog.infoworld.com/whurley/archives/2009/01/cloud_computing.html

[8] EDUCAUSE (2011). Things you should know about organizing files in the cloud. Retrieved on 7/17/2011 from http://www.educause.edu/ir/library/pdf/ELI7073.pdf.

[9] NIST SP 800-145. Retrieved on 7/10/2011 from http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[10] NIST SP 800-146. Retrieved on 7/10/2011 from http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[11] Diaz, V., Golas, J., & Gautsch, S. (2010). Privacy Considerations in Cloud-Based Teaching and Learning Environments. EDUCAUSE Learning Initiative.

[12] Katz, R., Goldstein, P., & Yanosky, R. (2009). Cloud Computing in Higher Education. EDUCAUSE.

[13] Information Assurance Undergraduate Program. Retrieved on 7/1/2011 from http://www.emich.edu/ia/undergraduate.html

[14] Information Assurance Graduate Program. Retrieved on 7/1/2011 from http://www.emich.edu/ia/graduate.html

[15] Information Assurance Ph.D. in Technology Program. Retrieved on 7/1/2011 from http://www.emich.edu/ia/phd.html

[16] *Principles of Information Security,* Third Edition, Whitman/Mattord, ISBN: 1-4239-0177-0, Publisher: Course Technology.

[17] *Shelly (2011). Systems Analysis and Design, 8th Edition: Video Enhanced. ISBN-10: 0-538-47443-2 ISBN-13: 978-0-538-47443-6 Publisher: Course Technology.*

[18] Computer Forensics – Investigating Network Intrusions and Cybercrime, EC-Council, Course Technology, 2010, Chapter 4

[19] Computer Online Forensic Evidence Extractor (COFEE). Microsoft Solutions Center for Government. Retrieved on 7/16/2011 from http://www.microsoft.com/industry/government/solutions/cofee/default.aspx.

[20] Gregory, P. (2010). CISSP Guide to Security Essentials, 1st Edition. Course Technology – Cengage Learning, 2010. ISBN-13: 978-1-4354-2819-5

[21] Snort (2011). Retrieved on 7/11/2011 from www.snort.org.

Samir Tout received the B.S. and M.Sc. degrees in Computer Science from The University of Western Ontario in 1992 and 1993, respectively. He received his Ph.D. in Computer Science from Nova Southeastern University in 2006. He has several publications in various topics, including Data Mining, Artificial Intelligence, Cloud Computing, and Software Architecture. He is currently an Associate Professor at Eastern Michigan University's Information Assurance Program under the School of Technology Studies.

Appendix A

Table 3: Implications of various cloud scenarios [10]

Scenario Effects (w)	Onsite Private Cloud (OPC)	Outsourced Private Cloud (OSPC)	Onsite Community Cloud (OCC)	Outsourced Community Cloud (OSCC)	Public Cloud (PC)	Picks
Network Dependency (2)	Limited	Reliable Communication link with provider	Inter-site communication links or use cryptography over a less controlled media	Same as OSPC with potentially multiple links	Depends on Internet, DNS Servers, ISP, router infrastructure, etc.	OPC, PC
Subscribers' need for IT Skills (1)	Traditional + New cloud skills	Access Policies*	Overall cloud configuration may be more complex and hence requires a higher skill level + Access Policies	Access Policies*	Access Policies*	OSPC, OSCC, PC
Workload locations (1)	Subscriber Control	Some visibility to subscriber	Workloads remain within participant organizations (may be subject to outsourcing policies)	Same as OSPC	For cost efficiency, workloads located where cost low. Subscriber typically cannot verify	OPC, OSPC
Risks from multi-tenancy (1)	Mitigated by restricting to internal. Vulnerable to malicious insiders	Same as OPC	Same as OPC but less restrictive due to more organizations	Same as OCC	Workloads may co-reside with others': reliability & security risk	OPC, OSPC, OCC, OSCC
Data import/export, performance (1)	Limited by onsite network capacity	Limited by network between subscriber and provider	Similar to OSPC	Same as OSPC	Refer to network dependency*	OPC, OSPC, OCC, OSCC
Potentially strong security (1)	Same level as non-cloud	Harden both security perimeters for Subscriber and Provider	Depends on the security of all the perimeters of the participant organizations	Same as OCC	Depends on Internet access control measures*	OPC, OSPC
Up-front migration	Significant-to-high	Modest-to-significant	Significant-to-high	Same as OSPC	Same as OSPC	OSPC, OSCC,

costs (3)	Cloud software installation: New/Converted Data Center, Scavanged Resources	To subscriber: negotiate SLA, upgrade network to connect to provider, switch from traditional to cloud, porting non-cloud, training				PC
Resources available (2)	Limited, fixed capacity	Subscriber can rent resources, fixed capacity	Limited	Same as OSPC	Public clouds generally unrestricted	PC

* Not covered in [10]. Comment is per our evaluation based on the NIST standard details.