Volume 4 No. 7, July 2014 ISSN 2223-4985

International Journal of Information and Communication Technology Research

http://www.esjournals.org

The Need for Strategic Planning Toward Adopting Cloud Computing in Higher Education

Samir Tout
Eastern Michigan University, Ypsilanti, MI, USA

ABSTRACT

In the July 2011 issue of this journal, I published an article that addressed the benefits as well as challenges that relate to the adoption of Cloud computing (CC) in the Eastern Michigan University (EMU) Information Assurance (IA) program. In that paper, I presented a roadmap for making that transition, which I had been trying to formulate, with valuable input from several colleagues at EMU. To complete such an arduous task, I went back to a set of the key courses in our program and evaluated the benefits that each of them can reap from transitioning IA into a cloud-supported infrastructure. After roughly three years of evaluation and validation of that roadmap, which was largely based on a quantitative assessment, this paper illustrates other important factors that we have explored, from a qualitative perspective. The hope is that other institutions currently in the process of, or even contemplating such a transition, can benefit from them. This paper will also include some refinements to the original proposal, based on certain developments that have re-shaped the industry since that publication. It culminates in a proposal for pursuing a cloud computing specific strategic plan that would align with the university-wide plan that is currently being developed.

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

1. INTRODUCTION

Cloud computing has managed to maintain one of the top positions in the technology "fad" wagon for the past few years. Largely based on the basic premise of reducing in-house Information Technology infrastructure and delegating a portion or all of that to a third party, cloud computing has evolved into a paradigm that holds great promise in revolutionizing the way we do business.

A natural grand child of the relatively defunct concept of Application Service Provider (ASP), which came out in the 1990's, cloud computing has regained the spotlight due to the considerable advancements in technology, which were not feasible in that era, but are now becoming available to the masses, such as much cheaper storage and blazing-fast Internet connectivity.

In November 2009, I presented at the ISECON'09 conference in Washington, D.C. about cloud computing. In that paper, which I had co-authored with two other EMU colleagues, we explored various aspects of cloud computing requirements in general, and as applied to a university setting in specific, with emphasis on its impact on cost and security [1]. I followed it with a publication in this very journal, in which I performed a quantitative assessment of the best cloud computing models for some of our key courses. I subsequently presented a roadmap for transitioning to such models based on that quantitative analysis. This paper reflects back on both publications and explores a more holistic approach to adopting cloud computing at EMU's IA, based on establishing a strategic plan that addresses other organizational factors that we had not considered.

This paper is organized as follows: Section 2 includes a brief definition of cloud computing, along with the case for and against it, as well as prior work done in this domain, including ours. Section 3 re-evaluates the potential for CC adoption at EMU by reflecting back on our roadmap that we presented in [22]. This section also uses a newly introduced course, which made it to the top of the list of popular courses since then, and served as an eye opener and a good case study for validating our previous roadmap. This section also covers a few university wide endeavors that may further re-shape our earlier approach. Section 4 provides a holistic approach that explores launching a qualitative analysis, which culminates in a strategic plan that takes into consideration the new developments discussed in Section 3. We end with our conclusion and plans for future work in Section 5.

2. DEFINITION AND DEVELOPMENTS IN CLOUD COMPUTING

2.1 Definitions and Relevant Literature

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling 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" [23]. Furthermore, in a more recent Special Publication (SP 800-145), NIST provided a concise definition of cloud computing by means of five essential characteristics, three service models, and four deployment models [24]. In [22], I explored NIST's SP 800-145, 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]. Furthermore, that study referred to NIST's SP 800-146, which explained cloud computing and provided recommendations for IT decision makers. This standard was later revised, in 2012 [25] and elaborated more on the various service models such as IaaS, PaaS, and IaaS then listed various open issues that I found very relevant to our situation in a university setting.

2.2 The Case for Cloud Computing

In a NY State CIO Conference in July 2009, the Vice President of EDUCAUSE, Richard N. Katz, spoke about "The Tower and the Cloud: Higher Education in the Age of Cloud Computing." He presented some interesting statistics that further demonstrated the importance of cloud computing and its prevalent role in modern organizations, including universities. He cited a poll that sensed how people felt about the role of cloud computing. In a nutshell, 74% of those polled thought that cloud services will have a great effect on higher education while 75% thought the same for their IT organization.

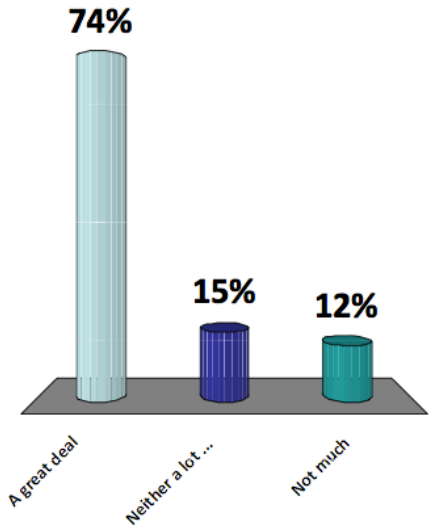

Fig. 1. How deeply will cloud services affect higher education? [12]

In a Cisco whitepaper titled "Cloud 101: Developing a Cloud-Computing Strategy for Higher Education" the authors explore the unique challenges that are faced in a higher education environment [26]. These included issues that we covered in [1] and [22], such as budget restrictions, varying systems that accommodate various program needs, and privacy. This paper also cited a CDW study [27], which demonstrated the prevalent support for cloud computing adoption in higher education along with the fiscal advantages that such migration provides to these institutions. For instance, with conventional in-house university-based infrastructure, downtime during off-peak school year times leads to under-utilization and therefore a substantial waste in power, cooling, etc. They also cited benefits, including increased efficiency and availability, simplification and standardization, and supporting innovation. They also included cases in which a university migrated to a multi-million dollar in-house data center, which according to their study, would require another massive upgrade a few years later, thus creating a long-term scalability challenge. They also cited a successful cloud case study where Berlin's University of Technology (TU) turned to virtualization of most of their IT infrastructure and therefore were able to achieve high scalability [26]. In [28], the authors stated "IT is finally catching up with the Internet by extending the enterprise outside of the traditional data center walls."

In [1], we cited several benefits of cloud computing and related how the Electrical Engineering and Computer Sciences Department at the University of California at Berkeley had a first-hand dealing with this matter whereby they indicated that their lab "has benefited substantially from the ability to complete research by conference deadlines and adjust resources over the semester to accommodate course deadlines." As adopters of cloud computing, they "were relieved of dealing with the twin dangers of over-provisioning and under-provisioning our internal datacenters." [29].

Furthermore, in [1], we indicated how complexity can be reduced with cloud computing and how the variety of disciplines that are inherent within a university learning environment impose the need for a multitude of hardware and software platforms that are installed on campus. This contributes to an increase in the complexity of such platforms and adds to the already challenging tasks of IT administrators, including those that manage networks and software. This can be even more detrimental with the recent budget cuts that affect the allocation of sufficient IT staff, thus overwhelming these administrators even further. The adoption of cloud computing is hoped to relieve these administrators from such burden. We also explained how cloud computing, if set up correctly, can serve the availability of the organization and support the normally challenging tasks of disaster recovery and business continuity.

In [22], I further elaborated on such benefits by exploring our IA-granted degrees, including undergraduate, graduate, and Ph.D. concentrations as well as the computing requirements for

various key courses in IA. I subsequently conducted a weighted factor analysis, which quantifiably assessed the model that is best fit for each of these courses, in an effort to apply that to similar ones in the IA program. However, as discussed later, this has proven to be insufficient, as it requires a more qualitative approach to that evaluation, which takes into account new developments, especially with a new lab-intensive course that may not align with these suggested models. Furthermore, it became evident that we had to expand the narrow focused quantitative analysis into a more comprehensive strategic plan that encompasses that as well as other university-wide endeavors.

2.3 The Case against Cloud Computing

In [1], we mentioned several obstacles that cloud computing faces before it can be widely adopted. We cited a research conducted by the IDC Enterprise Panel [30] which concluded that the primary concerns that IT personnel expressed at various levels are: security, performance and availability, integration with in-house IT and customizability, and finally Cost.

Security of enterprise information is one of the chief concerns that cloud-computing adopters have typically voiced. For instance, enterprise data can be placed in storage clouds and sent across the communication channels of a totally different country, with potentially different data privacy laws, and therefore may potentially expose sensitive data to the prying eyes of unauthorized individuals. This requires establishing strict Service Level Agreements (SLAs) in order to safeguard such information and prevent intrusion and data theft. This was addressed in [26] with the massive range of devices that proliferate university environments, such as BYOD (bring your own device) and the challenges that it brings in securing such range of devices. Another important challenge is the integration of cloud security controls with university-wide departments and their various applications. In other words, how seamless can this integration be and how effective will it be in maintaining the same level of information assurance of such applications, including their confidentiality, integrity, and availability? Another important question to be answered is in terms of application problem resolution and auditing, including how available will the application and system logs be to campus IT administrators who usually create their own scripts to scrape such logs and resolve outage problems. These questions cannot be easily answered with a pure quantitative study and therefore should be methodically explored in light of various pertinent factors, which we will discuss later.

Compliance is yet another challenge. There are existing laws that may question the fulfillment of cloud computing to their legal stipulations. These include the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Federal Information Security Management Act (FISMA), and the Family Educational Rights and Privacy Act of 1974 (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), which is even more pertinent to our academic institution. As it relates to these laws, several questions arise, including: how will the cloud vendor ensure the implementation of all the provisions within such government laws, such as the accreditation and certification of their information systems that is required by FISMA and whether the consumer of such cloud services is held responsible for such implementation. Furthermore, those engaged in the legal field can relate to a report that was generated by [31] in which the authors stated that "there are limits for institutions of higher education and research to legally safeguard the confidentiality and security of data once they engage cloud computing services from providers." This may be a deterrent for institutions that handle sensitive client information, such as a university hospital in which researchers conduct their experiments and store massive amounts of data about their patients, potentially in the cloud.

3. RE-EVALUATING THE ADOPTION OF CLOUD COMPUTING

3.1 Reflecting Back on the IA Cloud Computing Roadmap

In [22] I elaborated on the NIST standards, which established conventional definitions of cloud computing (SP 800-145) and divided it into five essential characteristics, three service models, and four deployment models. I also explored SP 800-146, which provided recommendations for information technology decision makers in terms of adopting cloud computing. I further covered the unique challenges that face higher education, especially in terms of compliance with laws and regulations, specifically FERPA. Subsequently, [22] contained in-depth analysis that pertains to the use of cloud computing at our Information Assurance program at EMU (EMU-IA). This entailed conducting a thorough overview of our degrees, our undergraduate, graduate, and Ph.D. curricula, followed by an attempt to determine the computing requirements for each of their associated key courses. It is worth noting that these courses were selected based on them being required in our degrees as well as based on enrollment data. In our undergraduate curriculum, the IA foundation group of courses turned out to be a good fit for an IaaS service model that can readily provision network resources. The IA management track, on the other hand, which contained courses that are less technical and more in the leadership and management areas were a good fit for a SaaS service model. The IA applied track, which mostly contained technical courses, such as computer forensics, was fit for a VM provisioning using SaaS. As to our graduate IA curriculum, the course that was explored therein, IA 642, Enterprise Security, aligned with a PaaS model as it explored CISSP security

domains and required various types of platforms for doing so. However, as discussed later, this is not set in stone, as different models may align better with the nature of other courses. The Ph.D. IA curriculum was determined to be a good fit for an IaaS model. Based on these determinations and the weighted factor analysis [22] which augmented the one that was conducted in [10], the recommendation was to start with a hybrid model by transitioning labs only for a few introductory courses like IA 103. This is while exploring the prospects of an outsourced private cloud [22]. Furthermore, the recommendation included opening a dialogue with other organizations within and outside of EMU to plan for a community or even a national cloud, as suggested in [4]. Later general recommendations stipulated moving to cloud computing based on a phased approach, with the IA transition being the first phase.

3.2 Re-Evaluating Earlier Analysis

After rolling out the analysis in [22], which was fairly quantitative, based on a weighted factor analysis that encompassed representative courses from our Information Assurance program, it became evident that we had to heed other relevant matters. A few new developments have reshaped the way we had originally approached our cloud computing adoption roadmap at our Information Assurance program in particular, and at EMU in general. This section will cover both and elicit how this delineated our new approach to CC adoption. This paper will cover a case study that is based on a relatively new course in Malware Analysis that we introduced in Fall 2012, which has slightly changed the landscape of our earlier analysis and served as an eye opener for other considerations to keep in mind when assessing the value, and model, of the best cloud computing architecture to fit in our academic institution. This section will also list a few other endeavors upon which EMU has embarked, which may also contribute to such re-evaluation of our prior approach.

3.3 A Case Study – Malware Analysis Course

3.3.1 The Introduction of IA 400

At the program level, the primary change was the introduction of a Malware Analysis and Reverse Engineering (MARE) course, IA 400, which is based on a new breed of a hands-on lab-intensive curriculum. MARE covers the fundamentals of malware analysis and established industry-standard approaches that are sanctioned by pioneers in this domain, like SANS [32]. IA 400 was first taught in Fall 2012 and soon became a flagship course that explores various types of malware specimen, including viruses, worms, Trojans, rootkits, as well as document-based malware. It also covers introductory best practices in conducting these analyses, along with the tools that support them. This course culminates in a group term paper in which students report their findings about a specific MARE topic after having conducted adequate research or a practical experiment that puts the above principles to practice. In both cases, students present their findings to the rest of the class and field their questions.

3.3.2 A Historical Overview of the IA 400 Environment

As a brief historical overview of the manner in which this course has evolved over the past two years, when we first rolled it out in Fall 2012, I spent a considerable amount of time with a fellow adjunct designing the proper configuration of the course materials, in an effort to maximize its benefit to our students and make it as effective as possible for classroom-based labs. We initially provisioned 25 physical hard drives that students had to "borrow" and kick-off at the beginning of every class to run the required daily labs. Each hard drive had a few Virtual Machines (VMs) that contained the required operating system along with the necessary tools to solve the problem presented in a given lab. We also deployed a hardware switch, which we would "hard-disconnect" before running malicious software, especially the known aggressive kinds, in an effort to isolate our next-door data center as well as the university network from its potential harm. After several hardware failures, it became evident that this is not an optimal setup and that we had to find another configuration that would be more conducive to a long-term stable environment for this course. In Winter 2014, we introduced an internal Torrent server, which students use to download the VMs at the beginning of class and could potentially save on a USB drive for later use. Of course, students were discouraged from deploying such VMs on their home network, especially when handling malware specimen from class. In fact, we made the classroom lab available to them throughout the week so that they bring in the VMs and work on them at their own convenience.

3.3.3 Analysis of IA 400

It is worth noting that IA 400 is considered to be a close peer to the IA 327 "Computer Forensics I" course which was explored in [22] as a potential representative of our Applied IA Track and therefore is assumed to fall under the same category that was determined to be a good fit for a SaaS model. It was suggested in [22] that this course would utilize a provider-provisioned VM that would be put at the subscriber's (IA) disposal.

There are several aspects of this course that serve as a good determinant, or at least a guideline, for the way we may be able to align it with a cloud computing service. Some of these are listed below and related to the proper CC service that could potentially make them optimal in serving the needs of the students and the course. The first point below is a major driving

force for others, but each has its own significant role in delineating our CC adoption approach.

a. Dangerous Specimen

The nature of practical labs, in which students could very well be handling a "live" (and potentially dangerous) malware specimen may present a challenge to CC adoption. This is especially true for external clouds whose providers may – rightfully – be concerned about the possibility of one of these specimen seeping into their networks and wreaking havoc therein. The fact that most of these providers use virtualization does not constitute sufficient re-assurance for them, as some of the specimen that are explored in this course may include virtual machine (VM)-aware and discovery capability that may threaten their very environments.

b. MARE Tools

A plethora of malware analysis and reverse engineering tools are explored and utilized as part of IA 400. Of particular use are those which provide monitoring capabilities and some that help dynamically debug the malware code. Although this is related to (a) above, this is more about the adequate setup of these tools, which work in tandom and are typically set up in a style that may be challenging to replicate in an external SaaS provider setting.

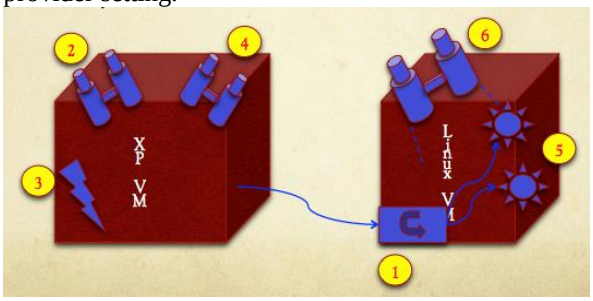

Fig. 2. IA 400 Lab Environment Example

c. Security and Privacy Concerns

In [22], one concern was raised regarding the use of EnCase or other forensics tools in IA 327 which may expose the sensitivity of data in real-world case studies. This was subsequently mitigated through either the obfuscation of data or the production of similar synthetic data. Unfortunately, this mitigation is not sufficient in the case of IA 400, since the use of live malware may not only geopardize that data, but even as determinental, it may threaten other cloud clients' data that may be sharing cloud-based storage. This is a serious concern that constituted a major determinant for our approach that we ended up adopting for this type of course, as stated later.

d. Students' Feedback

Another factor that I meant to capture in relation to our analysis was to obtain our student's insight, concerns, and suggestions as it pertains to this course. Another side-effect to obtaining this feedback was so to assess their level of comfort when it comes to various architectural models in support of this course, including cloud computing. For that purpose, after having gone through multiple variations, as stated earlier in the historical overview of this course, I rolled out a survey to MARE students. It presented several scenarios in which MARE course materials, including labs, would be available to them. Although the sample of respondants is still considered relatively low, I was able to gage an initial common theme, which indicates that the latest solution of having relevant VMs downloadable through a private torrent server and available for them to copy to a USB drive for later use were the most favorable options. This survey is still active as of this time, and I expect to report on it in about a year from this publication.

The above items have led us to conclude that, despite that previous quantitative analysis that we had performed on various key courses in our IA program, including IA 327, which is a peer of IA 400, we have to heed other considerations. Of particular relevance is the dangerous nature of malware specimen, the proper and effective deployment of malware tools, the security and privacy concerns, as well as student's feedback. Together, these suggest having a private cloud service that would incorporate our key VMs and make them readily available to students for working on the labs during and outside of class time. This is different than the original suggestion in [22] which was to deploy an external SaaS model for these types of courses.

3.3.4 The Cyber Security Awareness Committee

Another development, albeit at the university level, was the formation of a Cyber Security Awareness Committee (CyberSAC) that I helped co-found, toward the end of 2012, along with other key players across campus, including our IT, communication, and faculty development divisions. The main purpose of this committee was to spread awareness, after several reports that came out of our EMU IT division, indicated a considerable surge in spam activity that targeted various university personnel. Considering the ramifications of such threats, the inception of CyberSAC came as a natural response in order to educate our university community about the dangers of spam and take active measures to minimize its negative

impact. We have since conducted various activities toward these goals, including a "phish-me" campaign that faked the mass spamming of certain personnel with well-prepared and specially curated messages that culminated in providing direct (and private) educational feedback to those who fell for it. We also conducted various educational events, including a play that addressed spam messages and how to counter them. But one of the key activities, which is pertinent to cloud computing, as an offshoot of this committee, which we hope to roll out in our next academic year, is the preparation of a Cloud Computing Security and Awareness Workshop and survey. With the prevalent penetration of BYOD into the academic environments, and the necessity to ensure that they are streamlined with other existing systems, some of which are cloud-based while others are not, we felt compelled to conduct such a workshop and survey. The main reason is to gain a better understanding of the various cloud services that are currently at our campus community's disposal, and how to ensure secure interaction with them. Prior to that workshop, we will ask participants from various departments to bring in a list of key services that they currently use in serving their students, employees, and the university at large. This will help us build our knowledge base about such services and put us in a better position to make a more educated decision in our cloud services selection in the future.

3.3.5 Serving our Education First Mission

Other than being our main motto at EMU, Education First is a self-encompassing mission statement that has guided the way our personnel have approached various institutional undertakings. This includes the research that we typically conduct, the design of our curriculum, as well as our community engagement endeavors. One such example is the Raspberry Pi group [33] that I co-organized, toward the beginning of 2013, which now boasts about 140 members from various walks of technology fields. The group studies the Raspberry Pi, a credit-card size computer that serves as a Linux box and was initially launched by a non-profit organization in the UK, with the main purpose to educate the younger generation about technology and computer science. I originally founded this group to encourage our students to get actively involve in it, but that also evolved into using it as a tool to create projects that we could use to educate and trigger the interest of young, middle and high school students in various technology fields.

Furthermore, various really interesting projects have come out since the introduction of this platform, which ranged from sending a balloon up into the stratosphere with a Raspberry Pi and a camera to take screen shots of earth to the creation of full-blown security monitoring systems, to sprinkler system control, and more relevant to this paper, the ability to create a Pi-based cloud service that, despite its relatively minimal capabilities, compared to high horse-power servers that may be provided by external cloud providers, presents a viable option to explore, in addition to the ones that were listed in [22].

4. STRATEGIC PLANNING

As another improvement over the strict quantitative approach that was followed in [22], it is important to think strategically about cloud computing adoption and involve all key players from various university departments, including faculty, administration, and students. For that purpose, the following is an early attempt at establishing a cloud computing strategic plan, which heeds the various considerations from [22] as well as this paper, in an effort to make such transition based on a collective, and well-educated decision that takes into account different factors that may have a bearing on the success of such adoption. To that end, and as a start, we have launched a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis that will pave the way for this plan. Coincidentally, our current university administration was been working on producing a university-wide strategic plan, which would serve as a perfect incubator for our cloud-computing centered analysis. Our plan is to roll out a multitude of quantitative as well as qualitative research studies, some to be proposed as potential dissertation topics for our Ph.D. students, and have those feed into our CC strategic plan. Although we admit that this effort is still in its infancy, but since things move relatively slowly in academia, we would rather follow a longer yet methodical approach that takes into consideration EMU's specific needs, rather than a trial-and-error ad-hoc tactic that may eventually fail at the first test of time. Some of our students have already started working on cloud-related dissertation topics; one of these will be presenting his work, titled "Technological, Organizational, and Environmental Factors Affecting the Adoption of Cloud Enterprise Resource Planning (ERP) Systems" and will be defending it by the end of May 2014.

Below are the initial SWOT analysis areas that we plan to cover, based on a set of relevant questions that our research studies will attempt to answer. We will refine these as we roll this out to the larger university community. Of course, we will also leverage other similar advances that may have potentially been achieved by other sister institutions. But in an effort to make our approach as sound as possible, we would like to ensure that we reflect upon our own subjective matters first. Note that this is not a comprehensive list, but rather an initial attempt to compile key areas that would contribute to a more holistic cloud computing strategic plan at our institution.

Strengths Questions:

- What are the advantages in using cloud computing in support of student curriculum and learning systems?

- What are the advantages in using cloud computing for administrative systems?
- What are some of the existing capabilities that the university has, which may facilitate the adoption of cloud computing?
- How will the adoption of cloud computing help the university in achieving its full potential as an educational institution?
- How will the adoption of cloud computing help the university in achieving its full potential as a research institution?

Weaknesses Questions:

- Would the adoption of cloud computing at the university negatively affect the quality of students curricula and learning/administrative functions?
- What are some of the priorities the university has, which may hinder such an adoption?
- How will the adoption of cloud computing negatively impact the future of the university as an educational as well as a research institution?

Opportunities Questions:

- What are some of the opportunities that the adoption of cloud computing would provide to the university?
- How would the adoption of cloud computing make the university more competetive?
- Is the adoption of cloud computing timely in aligning with the larger strategic plan for the university?

Threats Questions:

- What are some of the threats that may jeopardize the mission of the university, should cloud computing be adopted?
- How would the adoption of cloud computing potentially present a threat to the key milestones in its long-term strategic plan?

5. CONCLUSION

This paper reflected back on [1] and more so, on the analysis that was conducted in [22], which was mostly of quantitative nature. New developments have surfaced since that analysis, including a new lab-intensive and unique course that may invalidate, if not at least revise, some of the recommendations in that paper. Since [22], several colleagues of mine and I have been working on some of the items that we identified in that study and decided to conduct a qualitative assessment of our readiness for adopting cloud computing in our IA program. This entailed taking a step back from the quantitative nature of our [22] approach and exploring the implications of introducing a course like IA 400, with its unique requirements and its sharply rising popularity. Our initial quantitative assessment in [22] suggested adopting a SaaS model for a similar peer course (IA 327) whereas, as discussed earlier, this may not be optimal setup for this type of course. Another development was to look beyond the Information Assurance program to university-wide initiatives that might very well have an impact on the overall decision of adopting cloud computing. This paper discussed two such endeavors: the CyberSAC committee initiative and the Raspberry Pi professional meetup group, each of which contributed a different perspective as it relates to cloud computing. This paper concluded by proposing a comprehensive approach, based on cloud computing-specific strategic plan that would align with the current institution's strategic plan. Key questions were formulated as part of a SWOT analysis, which would be a good first step toward such a plan. These questions are to be answered through various endeavors, including potentially becoming the subject of Ph.D. research work as well as possibly corroborating our findings with those of other similar institutions and industry-led research and whitepapers. The plan is to expand the work of the CyberSAC committee, which started as a security-focused entity and extend its role to lead the discussion about cloud computing adoption, as mentioned earlier. I hope to report back on our progress, which will include measurable steps that we plan to take in the next few years in order to complete the cloud computing strategic plan and put it to action.

Acknowledgments

I would like to thank Dr. Peggy Liggit, the director of the EMU faculty development center, Theodore Coutilish, AVP of university marketing, as well as Rocky Jenkins and Andrea Tanner from the EMU division of technology. This team has been tirelessly working with me throughout the past 1.5 years to address various security-related issues and are currently exploring topics related to cloud computing adoption.

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/EDUC

AUSEQuarterlyMagazineVolum/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.

[22] Tout, S. (2011). A Roadmap for Transitioning an Information Assurance Program and Others to Cloud Computing. The International Journal of Information and Communication Technology Research. Vol. 1, No. 3, pp. 128-138.

[23] Mell, Peter and Tim Grance (2009). "Draft NIST Working Definition of Cloud Computing." Retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, on August 28, 2009.

[24] Mell, Peter and Tim Grance (2011). "Draft NIST Working Definition of Cloud Computing." Retrieved from http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf on June 19, 2011.

[25] Badger, L., Grance, T., Patt-Corner, R., and Voas, J. (2012). "Cloud Computing Synopsis and Recommendations." National Institute of Standards and Technology, Special Publication 800-146.

[26] CISCO (2012). Cloud 101: Developing a Cloud-Computing Strategy for Higher Education. White Paper. Retrieved from http://www.cisco.com/c/dam/en/us/services/collateral/servi

ces/services-education/cloud_101_higher_education_wp.pdf, on May 18, 2014.

[27] CDW (2011). From Tactic to Strategy: The CDW 2011 Cloud Computing Tracking Poll."

[28] Reeves et al. (2009). Cloud Computing: Transforming IT, Burton Group Cloud Computing In-Depth Research, v1, April 20, 2009, p. 7.

[29] Armbrust, Michael, Armando Fox, et al. (2009). "Above the Clouds: A Berkeley View of Cloud Computing." Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley. Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf, on May 14, 2014.

[30] NIST, (2009). "Presentation on Effectively and Securely Using the Cloud Computing Paradigm v25". Retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v25.ppt, on August 29, 2009.

[31] Van Hoboken et al. (2012). Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act. Retrieved from https://confluence.terena.org/download/attachments/39846087/Cloud_Computing_Patriot_Act_2012_EN.pdf, on May 18, 2014.

[32] SANS (2014). Retrieved from http://www.sans.org/ on May 17, 2014.

[33] A2Rpi (2014). Retrieved from http://www.meetup.com/Ann-Arbor-Raspberry-Pi-Projects/ on May 10, 2014.

About Author

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, Security, and Software Architecture. He is currently a Professor at Eastern Michigan University's Information Assurance Program under the School of Technology Studies.