FACULTY USAGE OF CLOUD COMPUTING: THE CAPABILITIES AND RISKS

Walter W. Schilling
Software Engineering Program
Milwaukee School of Engineering

Abstract

Within the computer science arena, cloud computing has become a major topic of interest. Major computing corporations tout the advantages of such systems, including high reliability, scalability, remote availability, and other advantages. Major industries employ these types of systems in their daily business.

In the academic arena, cloud computing usage, aside from basic e-mail and web hosting, has been slower to develop. Some universities have outsourced email management and other limited administrative services. Outside of this area, the usage of cloud computing has generally been limited to individual faculty members using remote services. However, with the rapid escalation in cloud computing service availability, this is certain to change. This is not, however, without risk, both at an institutional and individual level.

This article addresses four aspects of cloud computing. First, it provides an overview of the services. Two major types of systems will be profiled, including file synchronization systems (DropBox, Ubuntu-One, etc.) and project management systems (GForge). The article will then address the impact upon an individual campus infrastructure. Beyond an IT aspect, the article will address the legal issues of using such a system, including the potential FERPA and DMCA ramifications to the institution and the faculty member. Lastly, a set of recommendations will be provided to faculty members who are interested in using cloud functionality in their teaching work.

Introduction

Cloud computing represents the latest evolution in computing architecture. By definition, cloud computing refers to "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management or service provider interaction."[1] Cloud computing, coupled with ubiquitous access through smart phones, tablets, and other internet enabled devices, has revolutionized software architecture and potentially will uproot traditional desktop computing.

Cloud computing does not represent new technology. Rather, it is the latest manifestation of large scale computing systems dating back to the 1970s when time shared systems were common. However, with the modern internet and reduced hardware costs, it is now much more practical to use large scale cloud computing systems in this manner. Thus, the birth of the cloud based paradigm.

Cloud computing from the corporate standpoint has gained popularity for several reasons. First and foremost, cloud computing services are very cost effective. While there may be membership fees, the costs of the systems tend to be lower than the comparable cost of deploying one's own system. Cloud computing systems are tremendously scalable. If more power is required, then more power can be purchased. Data stored in the cloud is constantly backed up because it is online. That does not mean it is impossible for data to be lost, as was evidenced by the Sidekick System failure in 2009[3], but there is a smaller chance

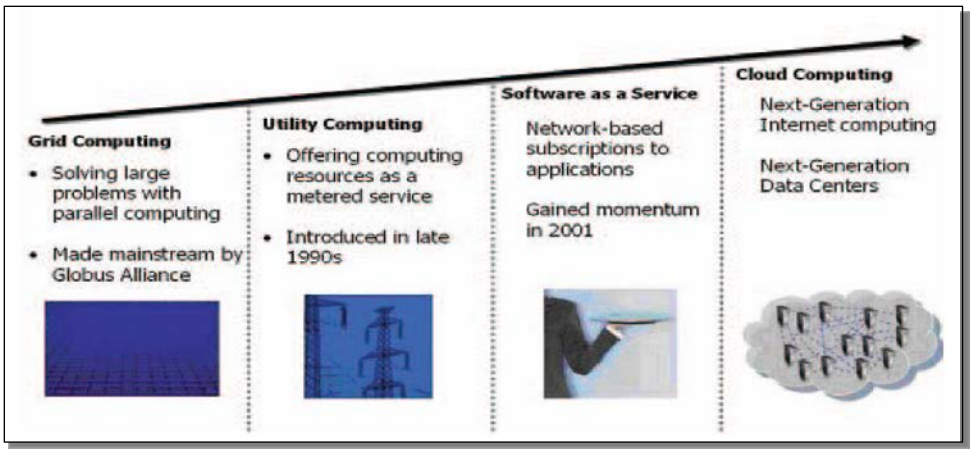

Figure 1: The evolution of computing towards cloud computing.[2]

than if one is responsible for one's own backups. Lastly, cloud computing reduces the need for a large IT support staff. Since the majority of the complexity is "in the cloud" the local staff can focus on servicing the support requirements of the local user as opposed to maintaining the operation of independent servers.

There are numerous cloud computing based systems available from service providers such as Amazon, Rackspace Cloud, Salesforce, Skytap, Microsoft and Google. And beyond these basic service providers, numerous applications have been developed to meet the specific needs of internet users. Commonly used cloud computing applications include Facebook, Flickr, Google Docs, Linked-In, Gmail, and others. Online storage systems have also become popular, allowing users to store their files in the cloud. Services such as Windows Live SkyDrive, DropBox, Box.net, Rackspace, and Egnyte offer the ability to store files in the cloud, backup local hard drives to the cloud, and set up file sharing between parties.

While cloud based computing has been rapidly adopted in certain industries, it has been slower to be accepted within the academic community. The one area where cloud computing has made inroads is in e-mail hosting. Major institutions in both the United States and abroad have outsourced their e-mail systems to cloud based companies[4,5,6]. Outsourcing e-mail systems, for either students or both students and faculty, offers greater storage capacity, high reliability, reduced cost, and additional features versus self hosted systems. Fostering this effort has been free services provided by Google and Microsoft.[7]

However, there are many systems that offer other services which might be useful for higher education, especially within the engineering field. Two such services which might be useful to faculty members include Dropbox and GForge.

Dropbox

Dropbox is a cloud based file hosting service which enables users to store, share, and synchronize files between multiple computers. Dropbox works by installing a file synchronization daemon on each desktop or laptop computer which is to be synchronized. As the user works, files which are stored into the directory are uploaded to the Dropbox system. All computers which are connected to the Dropbox service will automatically synchronize their files, so a change made on one computer will automatically propagate to the other computers as well. The computers need not be running the same operating system nor have the same configuration. Instead, each time the computer is booted, the system automatically synchronizes files at boot time. In addition to desktop and laptop computers,

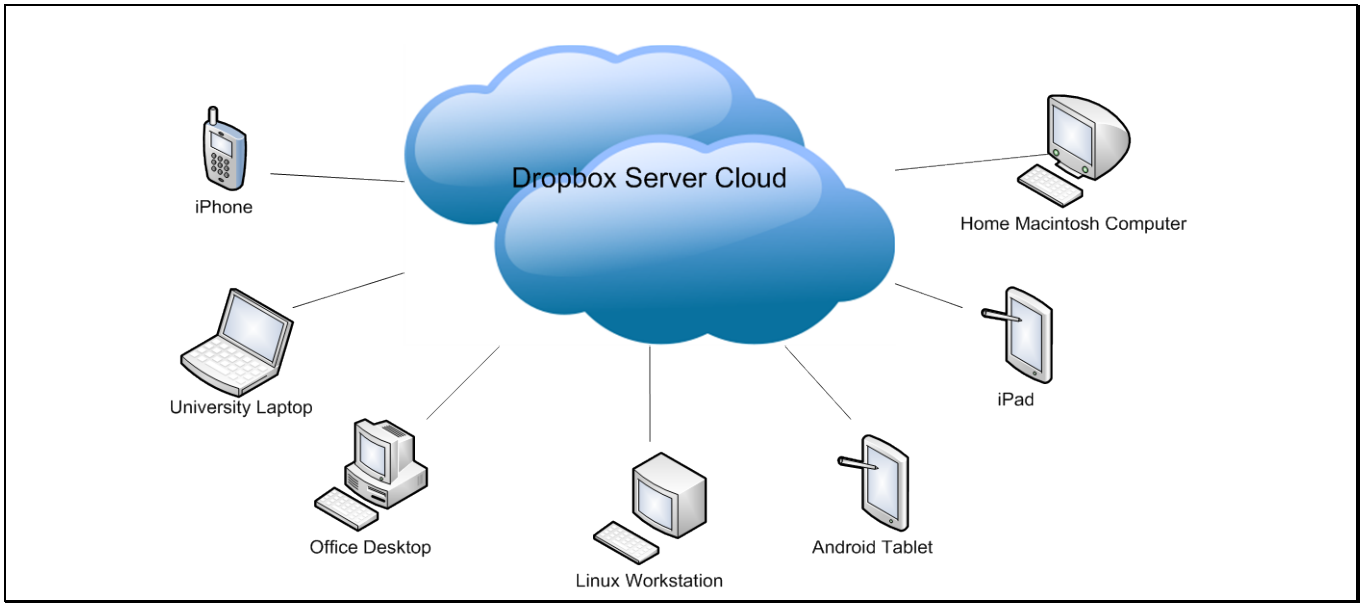

Figure 2 : Dropbox Cloud Architecture.

Dropbox allows users to access files through other means, with supported clients including Android, iPhone, iPad, and Blackberry. Dropbox stores its files in the cloud using the Amazon S3 on-demand storage system, and as of 2010 has 4 million users and stores over 20 billion files.[8]

Because of its nature, Dropbox offers a very convenient and automatic method for backing up critical data. Because the system automatically synchronizes directories, Dropbox serves as a defacto backup system. If one computer that a user has crashes, restoration is as simple as booting the new computer and installing the Dropbox client. Once the Dropbox client is installed, it will automatically restore the Dropbox directory to match that which is stored in the cloud.

A related feature of Dropbox is the ability to restore previous versions of a file. In addition to storing the current version of a file, Dropbox also stores previous versions of a file which have been edited over the past 30 days. An example of this is shown in Figure 3, where previous versions of an exam are listed. An additional add-on feature, Packrat, will keep an unlimited number of deleted files and old versions of the data from your directory. Thus, it is possible to potentially never lose an item of work.[9]

Dropbox also supports file sharing, webhosting, and online access as well.

Dropbox has a distinct advantage of being easy and inexpensive to install and use. The software is freely available, including both desktop and mobile applications. A basic plan, which allows a user to synchronize and store up to 2 GB of data is available for free, and larger subscriptions supporting 50GB or 100GB storage are available for $9.99 per month or $19.99 per month respectively. Annual plans are available for $99.00 and $199.99 per year as well, and there is a Dropbox for Team package which allows 5 users to share 350 GB of data for $795 per year.10 This package might be ideally suited for a small research lab with multiple graduate students.

In the academic realm, there are many convenient uses for the Dropbox system. At the lowest level, a faculty member can use the Dropbox service to automatically backup their research and classroom materials (lectures, handouts, gradebooks, etc.), preventing their

loss in the event of a computer crash. Given that up to 2GB of data can be stored for free, it is possible that the faculty member may not even need to pay for this service. A more advanced user may begin to use the more advanced features of Dropbox. A savvy faculty member may decide that they will not bring their university laptop home in the evening. Rather, they will access their files via a computer which is synchronized through Dropbox. This allows them to grade assignments and create lectures from home without hauling their laptop home. Upon arriving back in the office, the files will be synchronized and ready for the next day. Another faculty member might grade assignments on a plane flight and then enter them into their gradebook using their smartphone and DropBox's mobile device access.

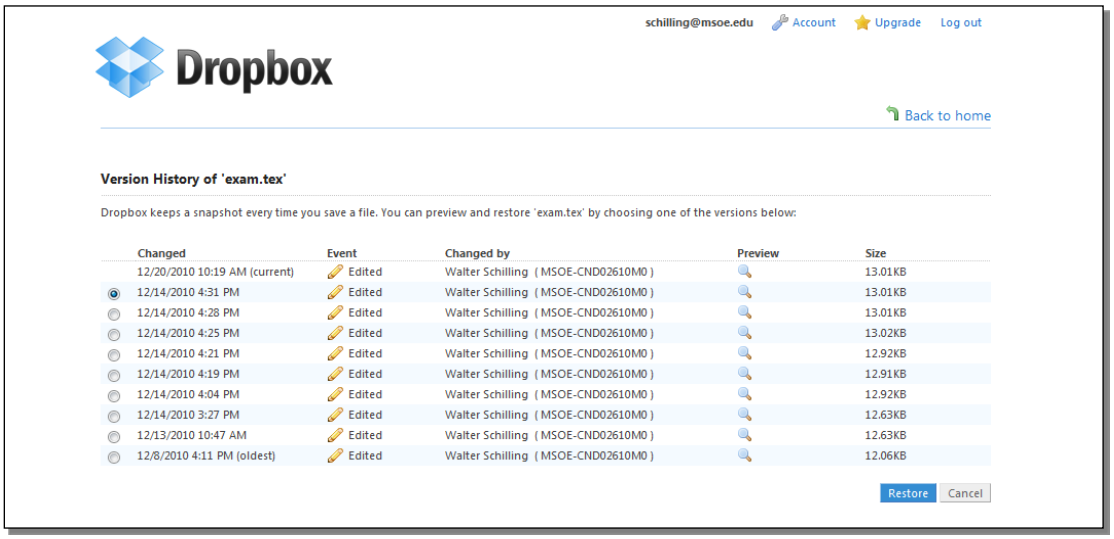

Figure 3: Sample Dropbox version history.

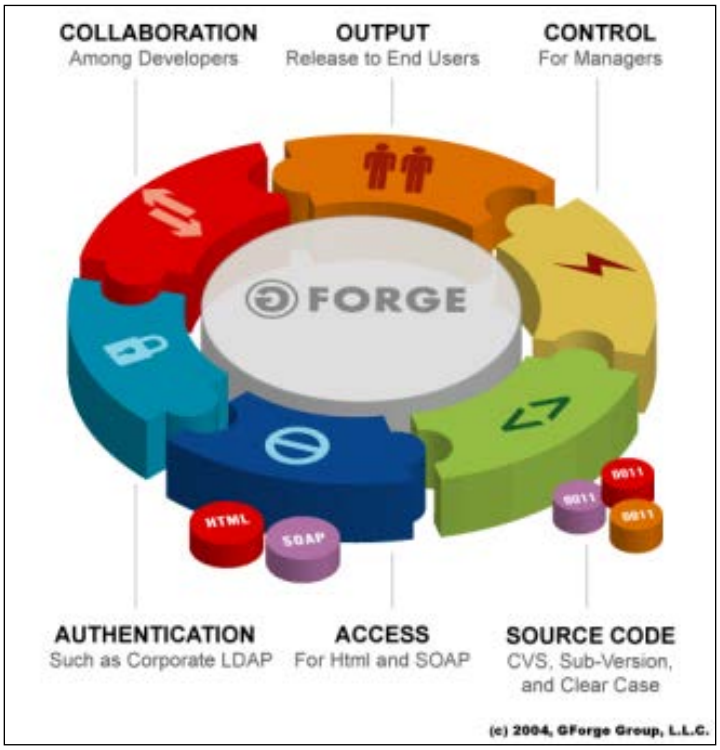

Figure 4: GForge system.

GForge

GForge is a collaborative software application in the cloud originally created for SourceForge. It includes multiple tools which engineering students find useful, especially for capstone projects. GForge integrates administrative tasks (user management, security, etc.), issue tracking, document storage, file storage, a wiki, and a subversion repository into a single online system. Students can then use the GForge system to store project artifacts as a project evolves.

GForge and related systems have been used in multiple environments for capstone projects.[11, 12] From a faculty standpoint, the GForge system allows a faculty member limitless access to analyze student work at any time. Any file which the student completes is available in the system and can be reviewed at any time. Faculty can also use the reporting capabilities of the system to determine project status and progress. Furthermore, because the system is online, an entire portfolio of the project is available, not just the final version.

As an open source project, GForge offers their software to anyone for free. More advanced packages are available for a fee which support more advanced reporting and additional capabilities. GForge also provides for cloud based hosting of projects. This service is free for those in an academic institution.

Impact upon campus systems

Previously, an overview of two cloud based systems was provided. The capabilities of the systems were discussed and potential faculty uses were provided. This segment is now going to focus on the impact upon campus systems of a faculty member using cloud based storage systems.

The first obvious problem that is introduced by the usage of cloud based systems is the issue of bandwidth and connectivity. Campus networks were initially designed to facilitate connections between campus machines and local servers. Network topologies have been optimized to allow the free flow of information from a campus server to local labs. However, as one moves to cloud based solution, large files are now transmitted on and off campus. This may present significant bandwidth problems to IT administrators. Their response may be to either throttle back on the bandwidth available to these sites in order to preserve other connections during the day or blatantly block them altogether. In the case of Dropbox, this problem can be potentially noticeable on Monday following a break in normal classroom activity. If the faculty member is turning on his / her computer for the first time in a few weeks, there may be a tremendously large number of files to synchronize. If you multiply this over many faculty, there is a distinct possibility of problems with bandwidth.

Firewalls also present a problem to cloud computing users. Dropbox in particular requires a secure connection and accurate timing information in order to verify the validity of the SSL certificate used for security. If the system clock on campus has drifted or is otherwise incorrect, it may not be possible to make a connection. In order to thwart other security concerns, IT administrators have also blocked access to the ports required by Dropbox to connect. Blocking these ports makes it impossible for your system to synchronize.

Cloud based systems pose potential security vulnerabilities in terms of computer viruses. By their nature, systems like Dropbox and GForge do not attempt to scan uploaded files for viruses. Rather, they expect that the user will follow proper precautions. Thus, if a user gets infected by a virus on their computer at home and interacts with one of these systems, there is the potential that the files in the cloud would become infected. In the case of DropBox, this then means that the files on all other synchronized machines would also become infected as the virus propagates. While this can

be managed, it certainly is a concern from the campus standpoint or the research lab standpoint. If not managed properly, one graduate student could infect an entire set of data files, potentially losing a significant amount of research work. And given the architecture of Dropbox, it may be very difficult to fully eradicate the infected files from the system.

Another issue that can come up is reliability issues. While in general it is likely that the cloud based systems will offer a higher reliability than a system deployed by a local IT department, this does not mean that failures are not possible. With Dropbox, a problem could develop if a faculty member did not bring their laptop home over the weekend to prepare for Monday morning's 8:00 lecture. Instead the faculty member prepared the lecture at home and assumed that Dropbox would synchronize upon arrival in the office. If the laptop computer is unable to access Dropbox due to any network problem on campus, then the file will not synchronize and the professor may not have lecture slides available. This can somewhat be circumvented by the usage of a mobile device interface in Dropbox's case, but it still is a potential issue.

Legal Issues

Previously the capabilities of cloud based systems and the impact upon campus IT departments have been discussed. These issues, however, are not the only issues faculty members must be concerned about when using cloud computing systems.

FERPA

From a faculty standpoint, the largest area of concern is FERPA. FERPA, the Family Educational Rights and Privacy Act, governs what information may be disclosed by faculty members and to whom it may be disclosed. With certain exceptions, it essentially means a faculty members may not speak directly about a student's achievement or disclose sample student assignments. It also places restrictions on how data is to be stored and who may have access to retained data.

The challenge of FERPA is how it applies to cloud computing systems. While by nature a cloud computing system does not directly disclose confidential information, material placed in the cloud can be viewed as out of the direct control of the professor and potentially accessible by non-university personnel (for example, a remote system administrator). This means care must be taken with FERPA protected materials. In the case of a course management system such as GForge, this would be student deliverables, student reports, potentially student comments (depending on how assignments are graded), and other materials. In the case of DropBox, this might be samples of student work being retained for promotion and tenure purposes, gradebooks, academic dishonesty filings, and other evaluations.

Dropbox, in its Security policy indicates that it has gone to significant extreme to protect the security of data stored within its system. Dropbox indicates that files are secured using the AES-256 standard, similar to that used by commercial banks and military organizations. The Amazon S3 cloud is protected using perimeter control beams, video surveillance, and other security staff. And, all transfers are protected using SSL encryption. Employees neither have the authorization or capability to view subscribers' files. Thus, in the context of modern computing, Dropbox has attempted to be as secure as it can be, and in many regards, is significantly more secure than an internal campus data center.

The questions remains, however, does FERPA allow such a disclosure? The FERPA regulations were updated on December 9, 2008, and include new language relating to the usage of contracts.[13] In specific, section § 99.31(a)(1) has been amended to allow the disclosure of education records without consent to contractors, consultants, volunteers, and other

outside parties to whom an educational agency or institution has outsourced institutional services or functions. Previously, the statute did not provide any guidance on the disclosure of educational records to non-employees. This change, however, allows disclosure to contractors provided " the contractor must ensure that only individuals with legitimate educational interests (as determined by the district or institution, as appropriate) obtain access to personally identifiable information from education records it maintains (or creates) on behalf of the district or institution. Further, in accordance with § 99.33(a) and (b), the contractor may not re-disclose personally identifiable information without consent unless the district or institution has authorized the re-disclosure under a FERPA exception and the district or institution records the subsequent disclosure."[13] Thus, it is permissible to use Dropbox as a service provider provided it has specified in its annual FERPA notification that it uses contractors, consultants, volunteers, etc. as school officials to provide certain institutional services and functions.

This allows an institution to subcontract with a cloud computing service for the storage of student records provided such a disclosure has been made. It is therefore perfectly legal for a faculty member to use such a system provided it is endorsed by the university.

However, the law is not as clear as to whether a faculty member themselves may use such a system to store student material. In the case of Dropbox, there are multiple cases that need to be individually interpreted and may have different issues. If a professor purchases the Dropbox service at an institution which uses external services, would it be legal to use the service for the storage of student information? If a professor registers for a free account would the interpretation be different? Is the professor required to disclose such usage to students? While Dropbox has been used in this example, the same issue applies to cloud hosted instances of GForge and other such applications.

DMCA

Beyond FERPA, the Digital Millennium Copyright Act of 1998 also potentially restricts what users can store in the cloud. Many textbooks now provide lectures, test questions, supplements, and other materials. These materials, however, are copyrighted. There is the potential that storing these materials on a cloud based system could potentially violate the terms of service for a cloud provider. Exceptions for so called "caching" or temporary storage may apply to such files, but the law is still unclear in this area as well.

In the case of Dropbox, it would be a clear violation of the terms of service to host copyright protected material through a web link. But the storage of material, provided it is properly licensed, is permissible. Thus, hosting the web slides provided by a textbook publisher within your Dropbox account would not be permitted, but storing a copy of them to lecture from would be permissible. Similar terms of service are also present within the GForge terms of service and most other cloud providers.

Retention

Another legal issue is the retention of data by a cloud computer service. In a traditional server environment, when a server is decommissioned, that data is no longer available, as the hard drives upon which the data was stored are scrubbed and backups may be destroyed. This model, however, is not practical in the realm of cloud computing. Since the data is distributed, it is not possible to guarantee that all data has been scrubbed from the original and backup materials. Records retention may also apply.

At the opposite realm, what happens if a service goes out of business in midterm. In the Dropbox model, where the system is merely backing up and synchronizing data, a service going out of business would merely be an inconvenience, as the service would no longer function but all of the data would be present and

replicated on each synchronized machine. However, a system such as GForge going out of business would significantly harm student's progress in a capstone project.

Practical Advice

In the previous section, an in-depth discussion of the legal issues and the challenges of using cloud computing for academic purposes have been discussed. In this section, practical advice will be provided as to how such a system can be used safely and effectively by a faculty member.

Classify Data Based on Risk

Before using a cloud based computing system, it is first necessary that one classify the data which they routinely store for criticality and confidentiality. A sample classification is provided in Table 1. Each professor and institution will have different types of data, and there may be institutional policies regards records and retention which must be followed.

In the example classification, the only reason a professor would not be able to use a cloud based system for public data is their own desire not to use such a system. This means that a professor certainly can store lecture notes, example problems, and other materials which they generate in such a system without any serious ramifications. There may be a few limited limitations on such a system (such as storing prepared lecture slides from a textbook), but for the most part, these issues can be overcome.

Protected Data also poses very few issues for a professor using a cloud based system. A professor has a very strong desire to keep protected data private. The exam or exam key could cause that professor significant problems if released to the student body in advance of the exam. However, this expose would not cause legal issues for the professor. The same applies to lab solutions. While published lab solutions would potentially make a given lab significantly easier for a given student, it would not cause long term issues.

Table 1: Sample document Classifications.

Classification	Description	Examples
Confidential Data	Data which might pose a significant legal liability for the professor or institution if it is disclosed.	Student grades Performance assessments Academic Misconduct reports Student Work
Protected Data	Data which would cause personal problems for an individual professor but might not yield legal problems if it is compromised	Exams Exam Keys Sample Lab Solutions Rubrics (if kept confidential) Grant Proposals
Public Data	This is data which, if compromised, will not have significant consequences Many of these items are either published or "effectively" published throughout the course	Lecture notes Course outlines Course outcomes Course syllabus Example problems

In many cases, cloud based systems actually offer an improvement over traditional systems. Traditionally, a professor might store protected data either on their own laptop and backup to a DVD, store the data on a flash drive, or store the data on a local network drive. In the first two instances, the material could easily be obtained from a student reading a misplaced storage device. The network drive might be accessed accidently by a student working in an IT environment. However, the likelihood of a breach of security for the cloud based system is lower, and the likelihood that such a breach would directly be knowledgeable to current students is even lower.

Confidential data provides the one area of concern with the usage of a cloud computing platform. The concerns purely rest with the manner in which the cloud contract is structured. In the event that an institution routinely uses contracted services and discloses this in their FERPA filing, then the usage of a cloud based service is acceptable.

However, the lack of contracted services by a university does not completely preclude the usage of a cloud based system for data storage. For example, a grade book is only a concern if it contains personally identifiable information. If a professor uses an appropriate randomization such that the gradebook which is stored in the cloud does not contain a student's name or official university identification, it may be possible for that material to be stored on a cloud computing resource without a FERPA concern. Thus, it may be possible for a faculty member to gain the advantages of using a cloud based solution while not overstepping the bounds of what is permissible under FERPA.

Encrypt All Confidential Data

It is generally a good practice, whether data is stored locally on a laptop or in the cloud, to encrypt all confidential data. Encryption involves the assignment of a password and application of an algorithm to ensure that only authorized users have access to read a given file. In the case of a laptop, encryption will protect the data present on the laptop in the event of the laptop being stolen or lost. Overall, there are many different approaches towards encrypting data, some of which provide for better security than others.

In the case of gradebooks, most professors use a spreadsheet. Unfortunately, the encryption mechanism built into most spreadsheet packages is better suited for protecting the files against inadvertent change than truly security the files. Microsoft Office, for example, uses a weak 128 bit RC4 scheme. This scheme suffers from a problem in that the key used for securing the documents is shared between versions. Thus, by having both a secured original document and a secured derivative document, it is possible to extract the password key relatively easily. Tools are also available online which are designed to aid in the recovery of data locked due to forgotten passwords. Unfortunately, these same tools can also be used to hack into these files if obtained.[15]

To properly encrypt a file, an external encryption package offers many advantages over the built in functions of Office and other readily available office packages. Simple encryption may be obtained by compressing the confidential data using WinZip or PkZip, which is significantly more secure than that built into an Office suite, and only storing the compressed version. Other open source software packages which are readily available include AES crypt and CC Crypt which offer secure storage alternatives. However, in the example of Dropbox, encrypting confidential material requires one to take the original file and encrypt it to the cloud storage solution. When reading the file, one must decrypt the file to an alternative location, modify the document, and then copy the encrypted version back to the cloud storage area. Decrypting the file to the cloud storage area would simply create an unencrypted copy of the file in the cloud based

repository, defeating the purpose for encrypting the file.

Purge Your Records of Unnecessary Files

Whether one is storing confidential information locally or in the cloud, it is advisable to periodically purge unneeded material from your repository. This may include deleting gradebooks for older courses, deleting sample student work after a sufficient period has passed, and deleting student assessments. By deleting this old material, the potential for an inadvertent disclosure is reduced. However, one does need to be careful, for there may be records retention statues which apply and require one to keep records for a fixed period of time. These laws vary between state and state and the policies vary significantly between institution and institution. And the records retention may be altered by a pending lawsuit or other legal action.

This is one area, however, where a cloud based system may prove difficult. This is especially true if someone has used a feature such as Dropbox's Packrat feature. With this feature, it is nearly impossible to guarantee that your records have been purged.

Archive Important Files Separate from Cloud Based Systems

The potential of a cloud based provider going out of business is a small but significant concern. Because of this concern, and because of the potential of a company disappearing without notice, it is recommended that you still keep small archival copies of important files in a separate location from the cloud based system. This will protect your effort in the event that a system goes defunct.

With some cloud based solutions, such as Dropbox, the nature of this backup is inherent based upon the architecture of the system. If Dropbox were to fail, the files still would be available on all synchronized machines. Rather, the mirroring and backup functionality of Dropbox would simply cease to operate. In the case of a system such as GForge, it would be very problematic, as the only copy of capstone project material would be lost by the cloud service provider going out of business. However, if students are using the cloud based system properly, they would not lose all work, as there would be copies of the latest work on their local machines. Rather, they would lose the ability to review previously made modifications.

Verify with your Chief Academic Officer Before Requiring Students to Use Cloud Based Systems

Prior to requiring students to use a cloud based system in a course, verify with the chief academic officer or other administration official that the usage of a system is permitted by university policy. It is one thing to use these tools for the storage of your class materials. However, it is extremely important that one verify that their usage is appropriate before requiring their usage in a course.

Conclusions

Cloud computing represents a rapidly evolving field. As such, there are many opportunities for this technology to be used for the benefit of faculty members. And, with caution, these techniques can be applied in a secure and legal manner. In many cases, the security and reliability of cloud computing solutions will significantly outperform campus based solutions.

This article has provided a high level overview of the capabilities of current cloud based systems, specifically highlighting the GForge and Dropbox systems. A discussion of the impacts on campus computing was then conducted. This was followed with a discussion of the legal aspects of using such systems in a campus environment, including FERPA and DMCA. Lastly some practical advice for faculty members who wish to use such systems in their teaching was provided.

Bibliography

1. P. Mell and T. Grance “NIST Definition of Cloud Computing v 15” Jul 10, 2009.

2. Tyrone Grandison, E. Michael Maximilien, Sean Thorpe, Alfredo Alba, "Towards a Formal Definition of a Computing Cloud," Services, IEEE Congress on, pp. 191-192, 2010 6th World Congress on Services, 2010

3. Daniel Eran Dilger. Microsoft's Danger Sidekick data loss casts dark on cloud computing. Apple Insider, 2009.

4. Andy Guess. When E-Mail is Outsourced, Inside Higher Ed, November 27, 2007.

5. Cynthia M. Hadden and Brian D. Voss, E-Mail: Paradigms, Options, and Outsourcing. EDUCAUSE Center for Applied Research Research Bulletin, November, 2006.

6. Alison Go, Colleges Outsource E-mail to Big Players, US News and World Reports By Alison Go, August, 2007.

7. Richard Otlet, Peter Tinson, Steven Bailey, Andrew Cormack and James Clay. Outsourcing Email and Data Storage Implications and opportunities. Universities and Colleges Information Systems Association (UCISA) and Universities UK, December 2008.

8. "There's room yet in the cloud". The Economist. August 24 2010. Retrieved 2010-12-12.

9. "What is Pack-Rat?". Dropbox FAQ. Dropbox, Inc.. Retrieved 2010-12-16.

10. "Dropbox Pricing Termsand Service". Dropbox. Dropbox, Inc.. Retrieved 2010-12-16.

11. Ge, Xun; Huang, Kun; and Dong, Yifei (2010) "An Investigation of an Open-Source Software Development Environment in a Software Engineering Graduate Course," Interdisciplinary Journal of Problem-based Learning: Vol. 4: Iss. 2, Article 6.

12. Evaluating the Use of Digital Product Repositories to Enhance Product Dissection Activities in the Classroom Matt Devendorf, Kemper Lewis, Timothy W. Simpson, Robert B. Stone, and William C. Regli, J. Comput. Inf. Sci. Eng. 9, 041008 (2009), DOI:10.1115/1.3264574

13. The Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR Part 99) , December 9, 2008.

14. Family Educational Rights and Privacy Act (FERPA), Final Rule 34 CFR Part 99 , Section-by-Section Analysis. December 2008. http://www2.ed.gov/ policy/gen/ guid/fpco/pdf/ht12-17-08-att.pdf Retriev ed 12/28/2010.

15. Robert Vamosi. Why Word and Excel password protection isn't safe. CNET Reviews, February 11, 2005.

Biographical Information

Walter Schilling is an assistant professor in the Software Engineering program at the Milwaukee School of Engineering in Milwaukee, WI. He received his BSEE from Ohio Northern University and his MSES and PhD from the University of Toledo. He worked in the automotive industry as an embedded software engineer for several years prior to returning for doctoral work. He has spent time at NASA Glenn Research Center in Cleveland, OH and consulted for multiple embedded systems companies in the Midwest. In addition to one US Patent, Schilling has numerous publications in refereed international conferences and other journals. He received the Ohio Space Grant Consortium Doctoral Fellowship, and has received awards from the IEEE Southeastern Michigan and IEEE Toledo Sections. He is a member of IEEE, IEEE Computer Society, and ASEE. At MSOE, he coordinates courses in Software Quality Assurance, Software Verification, Software Engineering Practices, Real Time Systems, and Operating Systems, as well as teaching Embedded Systems Software and other software and computer engineering courses.