

CLOUD-BASED EMAIL ARCHITECTURE FOR HIGHER EDUCATION INSTITUTIONS

Meena Srinivasan, University of the District of Columbia, msrinivasan@udc.edu

ABSTRACT

Higher education institutions have various ways to manage email communications and implement architecture that offers reliable service at reduced cost. This paper reports the results of study of email options used by higher education institutions. The two major email architectures that education institutions can implement are traditional on-premise and cloud services. This research finds that many institutions are shifting from on-premise to cloud based email which offer significant benefits as reduced cost and maintenance but have various risks related to privacy and confidentiality of student information. A hybrid model is a combination of on-premise and cloud services which offers benefits of clouds with low risks. This research will help higher education institutions who want to transition to the cloud understand risks associated with migrating and provides ways to balance the benefits and risks.

Keywords: Email, Cloud Computing, Cloud, Higher Education Institutions, Technology, Service Level Agreement

INTRODUCTION

Email is a critical form of communication between students, staff and faculty in higher education institutions (HEI). There are many ways institutions can manage email accounts of its users and HEI want to use an approach that reduces costs and improves services to students. The two broad ways that HEI can use to manage email of its users are: on-premise and cloud services. Another option available is use of hosted partners, but this approach is used more by business organizations. In this approach, the organization chooses a hosting partner to manage email but retains complete control of the data. The on-premise approach has been the traditional way email is managed by HEI. This approach has many challenges such as expensive investments, high storage, operating and maintenance costs. Due to these challenges, many institutions are in the process of shifting to cloud services. Most of the email services provided by major cloud providers are free and HEI can benefit by deploying email services to these providers.

Cloud services, similar to any new technology brings major challenges and opportunities. HEI can choose to shift email services to cloud or remain with on-premise architecture. Each of these choices has advantages and disadvantages and HEI need to assess their needs before choosing a suitable option for their email management. In the on-premise option, the institution manages the entire email infrastructure which can be expensive with high initial pricing, storage and maintenance costs. The reasons some HEI have shifted services to the cloud is low/no cost, use of latest technology offered by cloud providers and low maintenance. Temple University saved about one million dollars by shifting email services of its faculty and administrators to cloud [1]. However, the use of cloud services to manage email creates various challenges as loss of governance, litigation issues and security breaches. HEI must comply with FERPA (Family Educational Rights and Privacy Act) the federal law that must protect confidentiality and privacy of student records. The use of cloud to manage email services offers significant benefits but has risks that arise due to loss of control and a multi-tenant architecture. HEI can manage email with a hybrid approach that is a combination of on-premise and cloud services and thus maximize benefits of each approach.

The objective of this research is to study the different ways HEI are managing email services of it users composed of staff, students and faculty. This research briefly explores some of the challenges faced by HEI that deploy email services to the cloud. The email services used by 104 higher education institutions are studied and the different email management approaches used by them are investigated. The results of this research will help educational institutions understand risks associated with shifting to cloud and ways to balance the benefits and risks to implement suitable email architecture. The remainder of the paper is organized into five sections. The first section

presents a review of the literature on cloud computing and management of email services. The second section addresses the different email options available to HEI and discusses briefly the advantages and challenges of each approach. The third section presents the methodology of the research. The fourth section presents analysis of the results, challenges faced by HEI using cloud and recommends ways to mitigate these risks. The last section presents conclusions of this research.

LITERATURE REVIEW

One definition of cloud computing is the “delivery of scalable technology resources over the Internet, where services are implemented on hardware owned and managed by major providers [2]. Cloud services can be deployed in any of the following ways: Platform as a service (PaaS), Infrastructure as a Service (IaaS), or Software as a service (SaaS). The management of email is deployed as SaaS, where the cloud provider has total control of the system. There are many organizational, technical and legal issues associated with using services of cloud providers. The HEI must analyze and address these issues before a service level agreement (SLA) is negotiated with cloud provider. A SLA is an agreement between the cloud provider and the organization that deals with disaster recovery, data protection, security, termination, liability and related issues [3]. HEI need to choose a cloud provider who can offer solutions to majority of these issues as there is no complete solution to these risks. The main ways email can be implemented in HEI are on-premise, cloud-based or hybrid services. The use of cloud for email services creates many issues as security, data control and HEI need to make sure there are no violations to FERPA. Shifting to the cloud, means the organization will have more time and resources available for other responsibilities [4]. The University of North Carolina at Greensboro, the University of Texas at San Antonio, Arizona State University, University of Southern California, and Northwestern University are few HEI that have shifted to the cloud for email services [5]. The risks associated with privacy were reasons for the University of California Davis to terminate its service of Google for 30,000 students and staff [6]. The next section explains the different email management methods used by HEI and the challenges for each of these approaches.

MANAGEMENT OF EMAIL AT EDUCATION INSTITUTIONS

The email management methods available to HEI can be broadly classified as on-premise and cloud-based as shown in Figure 1. HEI can also manage email with a hybrid approach that is a combination of on-premise and cloud services. The hybrid approaches can be implemented in any of the following ways such as: hybrid-user, hybrid-function, hybrid-location or similar services and these are discussed in this section.

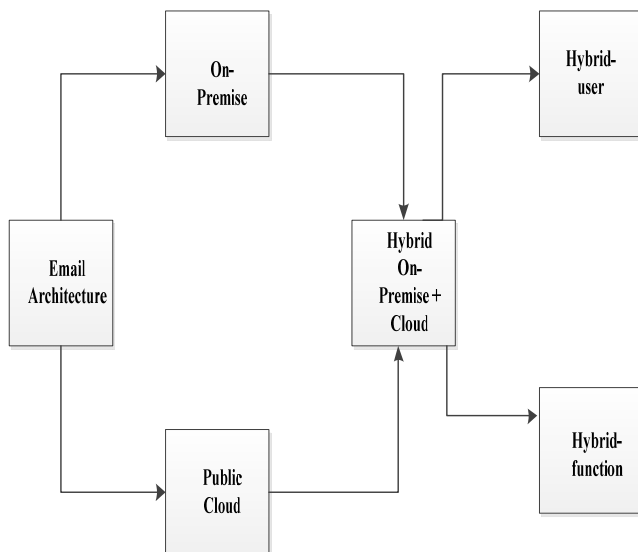


Figure 1: Email architectures for HEI

On-premise email

The on-premise approach for management of email has been the preferred choice for most businesses and education institutions. In this approach, all email functional services such as filtering, storage, archiving are maintained inside the organization. This option is secure and there are low risks related to privacy of student data. The main advantage of this approach is control of student data and the institution has its own disaster recovery, backup, security and related policies. The on-premise approach involves significant initial investments, ongoing maintenance costs, hardware and software costs and related expenses. Today, students need a lot of storage space and this approach has limitations and may not meet the demand of students. The many challenges with the on-premise approach have made HEI seek alternate approaches that are robust and meet the changing needs of the students. Many institutions are ready to shift to using cloud services which provides high storage, better service, rapid elasticity and scalability.

Cloud-based Services

Cloud based services are preferred by HEI that want to reduce costs, lower maintenance tasks and want to offer a robust agile email system for its users. HEI can deploy email to cloud providers such as Google or Microsoft who offer services to users for no charge. The significant benefits offered by the cloud, have caused many HEI to shift to using major cloud providers for email services where the entire email infrastructure is controlled by cloud provider. The loss of control and the shared infrastructure creates security and privacy risks for HEI. It is important that HEI find ways to address these challenges to benefit from the cloud. HEI are responsible for the security and integrity of student data but they are dependent on the provider to protect their valuable data.

A HEI using a cloud provider has no control over location of data and this causes legal and regulatory issues. Educational institutions may be locked-in with a particular cloud provider and it may be challenging to change vendors. HEI need to retain and present electronic information in legal investigations which can be complex in the cloud. Loss of governance, compliance, regulations are challenges as data in the cloud may be located in countries with different laws. HEI engaged in litigation issues may be subject to investigations and subpoenas. The electronic discovery process involves presentation of documents in litigation [7] and the cloud can make this process complex. HEI should ensure the cloud provider has a disaster recovery mechanism to protect and recover data in disaster. The cloud has many risks and the use of a hybrid model for email management allows HEI to balance the advantages of cloud with minimum risks.

Hybrid (cloud + on-premise) services

The cloud and on-premise email architecture can be combined to manage email thus maximizing the benefits of both with minimum risks. The pure cloud and the traditional on-premise approach used separately are not suitable to many education institutions. The hybrid approach can be used to obtain the benefits of both options where services are deployed to cloud in addition to on-premises email management. A hybrid architecture has many advantages, and can remove the drawbacks of pure cloud and on-premise approach. In a survey conducted by Trend Micro, 49% of the population is ready to adopt the cloud if they had the knowledge to secure their data [8]. This shows many organizations are ready to migrate entirely to the cloud if they knew ways to mitigate risks. The implementation of the hybrid approach will be an intermediate step for HEI where they can learn about issues with the cloud before migrating services.

The hybrid approaches can be implemented in any of the following ways such as: hybrid-user, hybrid-function, hybrid-location or similar services. Forrester surveyed 36 firms on email architecture, 20 plan to use a hybrid model, with inbound email spam and virus filtering as a cloud-based service [9]. This is an example of hybrid-function email management where email functions such as virus filtering, are migrated to the cloud. In the hybrid-location approach, email is deployed to the cloud for some locations and on-premise for other locations. In the hybrid-user architecture, the HEI may migrate email for some users to the cloud and maintain email for others on-premise for compliance purposes. An example is a HEI that can deploy student email in the cloud and maintain faculty and staff email on-premise. The hybrid-user approach is commonly used in HEI and other hybrid options are used more in businesses and hence will not be further discussed in this research. The advantages and disadvantages of the cloud-

based approach over on-premise for an organization are listed in Table 1 and Table 2 given below.

Table 1. Cloud vs. On-Premise: Advantages

Issues	On-premise	Cloud
Investments	High	Low
Costs	High	Low or no cost
Technology	Varies	Current
Storage space	Low	High
Maintenance	High	Low
Scalability	Not scalable	Scalable
Upgrades	Slow	Fast
Disaster recovery Business continuity	High cost; complex	Low cost; done by vendor
Deployment	Slow	Fast
IT needs	Complex	Simple
Agile	No	Yes

Table 2. Cloud vs. On-Premise: Disadvantages

Issues	On-premise	Cloud
Security concerns	Low	High
Location of data	Known	Unknown
Compliance issues	Secure	Insecure
Data control	Total control	No control
Multitenant architecture	No	Yes
Reliability	Yes	No
Inflexible SLA	No	Yes
Vendor management	No	Yes

METHODOLOGY

This research was conducted to study the email management methods used by educational institutions in the US. One hundred and three higher education institutions were randomly selected and the email architecture used by them was studied and analyzed. The email approach used by the HEI was found from the institution's website. The institutions selected were higher education colleges and universities and included small, medium and large, public and private institutions. The email management approach used by the HEI was classified as on-premise, cloud-based or hybrid-user services. The email management approach used for students, faculty and staff was surveyed for all the selected HEI. The name of the cloud providers was noted for all HEI. The population for this study is HEI that have well-defined email management approach. This research addresses the following questions.

1. What is the preferred email management approach for education institutions - cloud services, on-premise or hybrid-cloud? Can we claim at the 5% significance level that 33% or more HEI use cloud in some form to manage email? The cloud being a developing technology, if at least one-third of HEI use the cloud, one can conclude that it is favored by HEI for adoption.
2. Is the hybrid-user option more in use than pure cloud services? Would faculty and staff email be on-premise? Can we claim at the 5% significance level that less than 10% of HEI use cloud for all users – students, faculty and staff? Due to risks of the clouds and HEI not being adequately prepared to address these challenges, it is expected that less than 10% of HEI are ready to migrate faculty, staff and student email to the cloud.
3. What are the challenges faced by HEI in using cloud and how do HEI handle these challenges?

ANALYSIS OF RESULTS

The analysis of the study of 103 higher education institutions for email architecture shows the results in Table 3. The number of HEI using on-premise email architecture is 77%, pure cloud services is 5% and hybrid-user services is 18% (Figure 2). Majority of HEI use on-premise approach and are not using services of cloud for email management of faculty, staff and students. The reason for this are the challenges of the cloud as security, privacy and HEI are not prepared to address these risks. Higher education institutions are shifting to the cloud but clearly prefer the hybrid cloud model (78%) to pure cloud services (22%). The hybrid-user services are implemented so that faculty and staff email remain on-premise and student email is migrated to the cloud. HEI can realize the benefits of cloud by deploying student email to the cloud and minimize challenges such as compliance and governance by maintaining faculty and staff email on-premise.

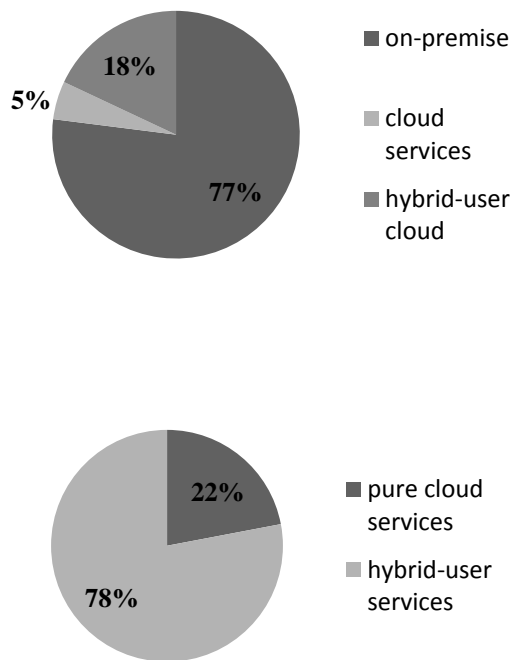


Figure 2. Analysis of email management at HEI

Table 3: Results of email approach used by 103 HEI

Email Model	Number of HEI
On-premise	79
Cloud (pure)	5
Hybrid-user cloud	19

The hypothesis testing to check if 33% or more of HEI use cloud in some form results in p-value of 0.993 at 5% level of significance. This means no definite conclusion can be drawn that the cloud is favored by more than one-third of HEI. However, the hypothesis generated to test that no more than 10% of HEI use cloud for faculty and staff has a p-value of 0.019. Hence one can claim at 5% significance level, many HEI are not ready to shift email of faculty and students to the cloud due to various challenges. From these results, it cannot be concluded that the cloud-based approach for email services is not a viable one. The two main cloud providers used by HEI are Microsoft and

Google. Institutions have to maintain confidentiality and privacy of student records and federal laws require there are no possible violations of FERPA. This can be achieved by negotiations with the cloud providers and education institutions and the SLA must include governance, compliance, retention policies, lock-in to avoid conflicts on legal issues if they arise. The resolution of any legal issues is the responsibility of the HEI.

How are HEI that have shifted to cloud dealing with challenges?

The deployment of email to the cloud has challenges and HEI can address them in different ways as listed below:

1. The HEI may be locked-in with a particular provider or the vendor may terminate its services anytime. HEI must be able to exit the cloud with ease, shift to another provider or migrate on premise. HEI should evaluate cloud SLAs and find providers who address these issues of lock-in, termination policies.
2. Compliance is a complex issue as various security and privacy laws have to be met. The location of data is not known and can be in a country with different laws for data protection and privacy. HEI must check with the cloud provider if data can be located easily when needed. .
3. A major challenge is electronic discovery when information has to be presented when a subpoena is issued. The HEI must retrieve the necessary documents and electronic discovery is complex process in the cloud and has to be addressed in the SLA.
4. Governance is the process by which HEI can ensure security in the cloud. Loss of governance is a concern in the cloud as HEI must comply with laws, regulations and various issues as ownership of data.
5. The cloud provider needs to have business continuity and backup plans. HEI need to make sure that the cloud provider has a disaster recovery mechanism to retrieve data.
6. The cloud provider must have ways to address deletion of data, security breaches and inform the HEI of any security breach.

RECOMMENDATIONS and CONCLUSION

The following are some recommendations so HEI can further benefit from the cloud and mitigate risks. Many of the cloud providers do not have experience in providing services for HEI. The HEI can use a third party to ensure that the terms of service with the provider includes details such as license, termination, liability, privacy and ways to address breaches. The HEI has no control in the cloud, and has to trust the cloud vendor. HEI should evaluate different cloud SLAs and find the appropriate provider who can provide sufficient SLA terms. HEI should have policies to educate all users that e-mail can be insecure and ensure that faculty, students and staff understands email practices. HEI can collaborate and form a baseline of required SLA agreements and negotiate with providers to create an agreement that meet their needs. Google was willing to negotiate and assume responsibility and address FERPA concerns in faculty and staff email after a number of schools approached it [10].

The ideal way to benefit from cloud is a blend of cloud services and on-premise options and this choice requires a balance between security and costs. The results show that education institutions prefer on-premise approach though they are keen to adopt the cloud. The results also indicate that the choices for staff and faculty can be different from those for students. The cloud offers major benefits as high storage, low maintenance and the cost of cloud deployments is lower than those of traditional on-premise email. Cloud computing is a new technology and educational institutions are ready to adopt the cloud if there are solutions to complex issues of security and privacy.

REFERENCES

1. Young, R. J. (2009, September 21).Colleges Warily Turn Sensitive E-Mail Over to Outside Companies, *The Chronicle of Higher Education*, Retrieved July 12, 2011, from <http://chronicle.com/article/Despite-Risks-IT-Officials/48503/>
2. Educause, (2009, August). *7 things you should know about cloud computing*, Retrieved July 11, 2011 from <http://net.educause.edu/ir/library/pdf/EST0902.pdf>
3. Jansen, W. & Grance, T. (2011, January). Guidelines on Security and Privacy in Public Cloud Computing, *NIST Special Publication*, Retrieved July11, 2011 from http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

4. Kundra, V. (2011 Feb). *Federal cloud computing strategy*, Retrieved July 11, 2011 from <http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf>
5. Inside Higher Ed, (2007, November 27). *When E-Mail is Outsourced*, Retrieved July 12, 2011 from <http://www.insidehighered.com/news/2007/11/27/email/>
6. Carter, D. (2010, June 3). Some colleges have second thoughts on Gmail *ecampusnews*, *Ecampus News*, Retrieved May 12, 2011, from <http://www.ecampusnews.com/technologies/some-colleges-have-second-thoughts-on-gmail/>
7. Alistair B. D. (2005, Feb). Understanding Electronic Discovery and Solving Its Problems, *56th Annual Program on Oil and Gas Law, The Center for American and International Law*, Houston, Texas, Retrieved May 12, 2011, from <http://www.brsfirm.com/publications/docs/00037W.pdf>
8. Subramanian, K. (2011). Hybrid Clouds, *Trend Micro*, Retrieved July 12, 2011 from http://us.trendmicro.com/imperia/md/content/us/pdf/solutions/enterprisebusiness/cloudjourney/wp01_hybridcloud-krish_110624us.pdf
9. Schadler, T. (2009, January 5). *Should Your Email Live In The Cloud? A Comparative Cost Analysis*, Forrester Research, Retrieved July 11, 2011, from http://www.forrester.com/rb/Research/should_email_live_in_cloud_comparative_cost/q/id/46302/t/2
10. Mitrano T (2009 August). *Outsourcing and Cloud Computing for Higher Education*, Retrieved July 11, 2011, from <http://www.cit.cornell.edu/policies/cloud/challenges.cfm>