ATHLETIC TRAINING EDUCATION JOURNAL

www.nataej.org
ISSN: 1947-380X
DOI: 10.5608/0703137

COLUMN:
EDUCATIONAL TECHNOLOGY

The Use of Cloud Technology In Athletic Training Education

Dennis Perkey, EdD, LAT, ATC
Arkansas State University, Jonesboro, AR

As technology advances and becomes more portable, athletic training educators (ATEs) have many options available to them. Whether attempting to streamline efforts in courses, or operate a more efficient athletic training education program, portable technology is becoming an important tool that will assist the ATE. One tool that allows more portability and efficiency is cloud computing. Cloud computing is not a new concept; it has been around for over a decade. Recently, cloud computing has become more popular with added user friendly versions that meet the need and demands of the increasing number of users. What makes cloud computing so popular is the portability it provides the user. At its basic function all that is needed to use this technology is a device that is able to connect to the internet and internet connectivity. The intention of this paper to provide an overview of cloud computing, describe the different types of cloud computing, and explain how ATEs can use cloud computing to enhance their educational practices.

What Is Cloud Computing?

Many definitions of cloud computing exist. A definition by Ambrust and Fox[1] define cloud computing as "applications delivered as services over the internet and software housed in data centers that provide services."[(p.50)] However, the most widely accepted definition is provided by The National Institute of Standards And Technology (NIST). The NIST is responsible for developing standards and guidelines under The NIST Federal Information Security Management Act (FISMA) of 2002.[2] The NIST defines cloud computing as:

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[2(p.2)]

The NIST[2(p.2)] indicates in that in order to be considered a cloud, the service must have the following five essential characteristics to be considered a cloud for computing:

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

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

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

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

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

In order for the cloud user to gain access to the cloud's applications, the owner of the cloud must decide how to deploy the cloud so the user can gain access to the information they need to store. The NIST lists four deployment models that describe how information on the cloud is stored. The deployment models include:

About the Column Editor:

Dr. Perkey is an Assistant Professor and the Athletic Training Education Program Clinical Coordinator at Arkansas State University, Jonesboro. Please address all correspondence to dperkey@astate.edu.

Full citation:
Perkey D. The Use of Cloud Technology In Athletic Training Education. *Athl Train Educ J.* 2012;7(3):137–139.

2) Community cloud- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg, mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

3) Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

4) Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (eg, cloud bursting for load balancing between clouds).[2(p.3)]

The community and hybrid cloud go beyond the scope of this paper and the focus will remain on public and private clouds, which are currently the most popular cloud services used by ATEs.

The owner of the cloud must also consider the type of service the cloud will provide the user. The NIST lists three different types of service models for cloud computing. Service models describe how the cloud services are delivered to the user, what software can be utilized, and the type of data that can be accessed by the user. NIST identifies three types of service models:[2]

1) Software as a Service (SaaS) - Allows the cloud user to run the cloud's infrastructure through various devices (ie, desk top computers, laptop computers and mobile devices). The application can be accessed through a web browser or a program interface. The cloud user does not control the network or the server, but on some occasions a designated user may control access to specific areas by other users.

2) Platform as Service (PaaS) - Allows the cloud user to add other applications to the cloud for other users however, the user does not have control of the server, but can control the application's operating system and deployment options.

3) Infrastructure as a Service (IaaS) - Allows the cloud user to deploy external software which can include additional applications and operating systems. The cloud user does not control the cloud but can control storage, operating systems, and may have limited control over networking applications.

CLOUD SECURITY

A major concern with cloud computing is the security of the information that is stored on the cloud. Maintaining the security of a cloud is the responsibility of the cloud provider. Providers offer different levels of security, attempting to meet the needs of the organization it serves.

The International Organization for Standardization (ISO) requires cloud vendors to implement security controls that are specifically designed to ensure that the products are safe, reliable, and of good quality.[3] Specifically, the ISO offers two standards that should be met by cloud computing vendors. The ISO 27001 is responsible for setting requirements for the application of security controls that can be customized to fit the needs of the organization, and the ISO 27002 intention is to meet the individual needs of an organization based on the results of a security risk assessment.[3,4]

A reliable and secure cloud provider will hold a certification that verifies that the services offered meets the ISO standards. The certification the cloud user should look for when deciding on which cloud provider to use is the SAS Type II certification. This certification is an independent, third party audit that is designed to provide verification that a service organization's policies and procedures are correctly designed so the consumer is protected in case there is a security breach.5 Breaches in security are a major concern, and these standards and certifications should give the cloud consumer peace of mind when deciding on which cloud service to use.

The Debate Over Cloud security

A debate exists between which type of cloud service offers the best security. One theory is that organizations that operate public clouds provide the best and most security because of the type and the amount of information that is stored in these clouds. Public clouds are typically owned by larger organizations and therefore will typically employ the latest and most expensive security technology. Due to the size of these organizations, they have the resources to hire the better and more qualified personnel to operate and maintain this type of technology.

Others claim organizations that operate private clouds offer the best security because they function for specific organizations, thereby limiting the type of data that is stored. Depending on the size of the organization this may or may not be the case. Large corporations who store large amounts of personal data on private clouds may be more prone to attacks or security breaches on their cloud because of the type of information housed within the cloud. Also, private clouds must exercise caution and be alert from the possibility of internal cloud attacks coming from within their organization.[6] This threat requires extra security that only authorized personnel within that organization can have access.

Athletic Training Education in Private Clouds

Athletic Training Education (ATE) has entered into the world of cloud computing with the development of ATrack and E*Value™ data management systems. Both cloud systems include the five essential characteristics of a cloud as described by the NIST,[2] and both systems are delivered through a private cloud in a SaaS format.

ATEs who use these programs have the ability to store and track important data that previously required many clock hours to manage. This data includes the current athletic training education program course matrix, individual student files, evaluations of both athletic training students and

clinical instructors, and the latest calculations of student clinical hours. These two clouds make it possible for the ATE to access and update information from their office computer or mobile device.

Clinical instructors also benefit from cloud computing. Clinical instructors can enter data into the cloud updating students' performance by logging into the cloud using their own private password. Clinical instructors can also verify clinical hours entered by the athletic training students, and enter proficiencies that have been completed by their athletic training students.

Athletic training students benefit from cloud computing by keeping track of their completed proficiencies, clinical hours, evaluations, and other important data such as advising records the ATE has allowed the students to track. This data that is stored in the cloud may also serve as a portfolio for students who need show a record of professional development while enrolled in an athletic training education program.

Conclusion

Cloud computing is a very broad topic that covers many areas. The intent of this column was to describe the different types of cloud computing and how ATE's can use cloud computing to enhance their educational practices.

Cloud computing will continue to develop and improve. As the demand for cloud services continue to increase the consumer base will continue to expand and demand more function from their cloud services. ATE's should embrace this technology and what it has to offer the educator as well as the student. Security should be a concern of both the ATE and the student, however, there are governmental standards and independent audits are in place to protect the consumer.

As athletic training education moves forward each individual athletic training education program and ATE will have to evaluate their needs to see if and which type of cloud computing will be beneficial to their situation. Future research on cloud computing should look at the different types of cloud services and how each can benefit both the ATE and the student.

REFERENCES

1. Ambrust M, Fox A, Griffith R, et al. A view of cloud computing. Communications of the ALM. 2011;53 (4):50-58. http://cacm.acm.org/magazines/2010/4/81493-a-view-of-cloud-computing/fulltext. Accessed June 11, 2012.
2. Mell P, Grance T. The NIST definition of cloud computing Recommendations of the National Institute of Standards and Technology. 2011:2-3. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Accessed June 11, 2012.
3. ISO (1). ISO/IEC 27001: 2005. Information technology-Security techniques Information security management systems-Requirements. 2008; http://www.iso.org/iso/catalogue_detail?csnumber=42103. Accessed June 25, 2012.
4. ISO (2). ISO/IEC 27001:2005. Information technology-Security techniques Information security management systems-Requirements. 2008; http://www.iso.org/iso/catalogue_detail?csnumber=50297. Accessed June 25, 2012.
5. SAS 70. Introduction to SAS 70 Type II Audit. http://www.sas70exam.com/services/type-ii-sas-70-audit/. Accessed June 25, 2012.
6. Simmonds, D, Wahab, A. Public Computing vs. private cloud computing: How security matters. http://www.cameron.edu/uploads/23/6c/236c70c76e3f71fc865cda0e2936cc2b/4.pdf. Accessed June 26, 2012.