Security Concerns and Remedy in a Cloud Based E-learning System

Md. Anwar Hossain Masud[1,*] , Md. Rafiqul Islam[1], and Jemal Abawajy[2]

[1] School of Computing and Mathematics,
Charles Sturt University, Albury, Australia
{manwarhossain,mislam}@csu.edu.au
[2] School of Information Technology,
Deakin University, Australia
jemal.abawajy@deakin.edu.au

Abstract. Cloud computing is an emerging technology and it utilizes the cloud power to many technical solutions. The e-learning solution is one of those technologies where it implements the cloud power in its existing system to enhance the functionality providing to e-learners. Cloud technology has numerous advantages over the existing traditional e-learning systems. However security is a major concern in cloud based e-learning. Therefore security measures are unavoidable to prevent the loss of users' valuable data from the security vulnerabilities. This paper investigates various security issues involved in cloud based e-learning technology with an aim to suggest remedial in the form of security measures and security management standards. These will help to overcome the security threats in cloud based e-learning technology. Solving the key problems will also encourage the widespread adoption of cloud computing in educational institutes.

1 Introduction

E-learning is a form of learning created by combining digitally delivered content with learning support and services. E-learning systems usually require many hardware and software resources. Educational organizations cannot afford huge investments to obtain these resources. In past three decades, the computing world is based on the Internet, featured by the rapid development and application of computer technology. The cloud computing model is one of the very important shapes of a new era. This technology is based on the distributed computing, parallel computing, grid computing, Virtualization technologies; property- based remote attestation technologies, etc. Cloud computing is the best solution as it delivers the computing resources (hardware and software) as a service over the internet [1]. It provides resources and capabilities of information technology via services offered by CSP (cloud service provider). It is a way to increase the capacity or add capabilities dynamically without investing in new

[*] Corresponding author.

T. Zia et al. (Eds.): SecureComm 2013, LNICST 127, pp. 356–366, 2013.

infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. As cloud computing has become a research hotspot among modern technologies, researchers pay more attentions to its applications. When cloud computing is applied in the field of education, a lot of problems had been studied, such as the technology for future distance education cloud, teaching information system [2] [3] [4], the integration of teaching resources [5], and teaching systems development [6]. In integration of e-learning and network, emphasis is placed on building of software and hardware platform in e-learning system, functional structure, network security management and training, information technology integration to teaching [7], campus network environment [8], online education[9] and semantic web technologies-based multi-agent system [10] [12].

Cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. This paper examines security issues associated with e-learning. It investigates the more popular e-learning standards to determine their provisions and limitations for security. This paper also focuses on the basic way of cloud computing development in relation to e-learning, growths and common security issues arising from the usage of cloud services.

The rest of the paper is organized as follows. Section 2 describes traditional e-learning to cloud e-learning. Section 3 describes privacy and security in e-learning while section 4 explains the security concerns in cloud computing. Section 5 describes cloud based possible attacks, section 6 describes the proposed identity authentication in cloud based e-learning and section 7 is the conclusion.

2 From Traditional E-Learning Network to Cloud E-Learning

E-learning is an Internet-based learning process, using Internet technology to design, implement, select, manage, support and extend learning, which will not replace traditional education methods, but will greatly improve the efficiency of education. As e-learning has a lot of advantages like flexibility, diversity, measurement, opening and so on, it will become a primary way for learning in the new century as depicted in Fig. 1.[20]

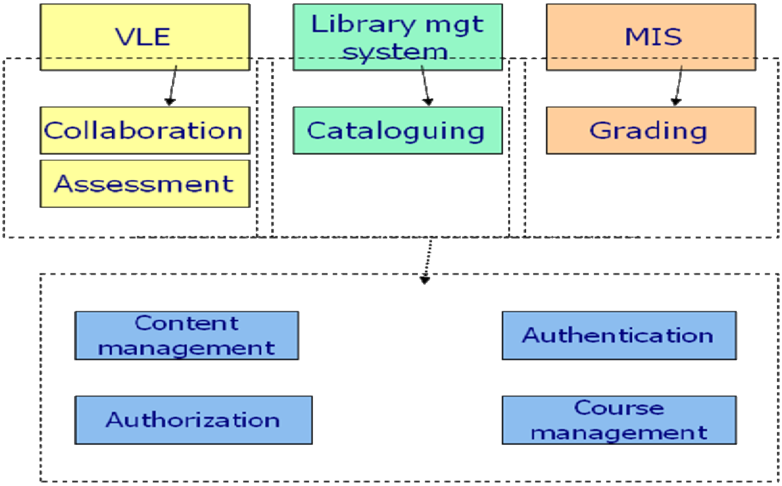

Fig. 1. Architecture of a simplified Learning System

Mendez [11] illustrates that in traditional web-based learning mode, system construction and maintenance are located inside the educational institutions or enterprises, which led to a lot of problems, such as significant investment needed but without capital gains for them, which leads to a lack of development potential. In contrast, cloud-based e-learning model introduces scale efficiency mechanism, i.e. construction of e-learning system is entrusted to cloud computing suppliers, which can make providers and users to achieve a win-win situation. The cloud-based environment supports the creation of new generation of e-learning systems, able to run on a wide range of hardware devices, while storing data inside the cloud. Ouf [19] has presented an innovative e-learning ecosystem based on cloud computing and Web 2.0 technologies. The article analyses the most important cloud-based services provided by public cloud computing environments such as Google App Engine, Amazon Elastic Compute Cloud (EC2) or Windows Azure, and highlights the advantages of deploying e-learning 2.0 applications for such an infrastructure. The authors also identified the benefits of cloud-based e-learning 2.0 applications (scalability, feasibility, or availability) and underlined the enhancements regarding the cost and risk management.

Chandran [17] focused on current e-learning architecture model and on issues in current e-learning applications. The article presents the Hybrid Instructional Model as the blend of the traditional classroom and online education and its customization for e-learning applications running on the cloud computing infrastructure. The authors underline the e-learning issues, especially the openness, scalability, and development/customization costs. The existing e-learning systems are not dynamically scalable and hard to extend integration with other e-learning systems is very expensive. The article proposed the hybrid cloud delivery model that can help in fixing the mentioned problems. In this article a new paradigm is highlighted in educational area by introducing the cloud computing in order to increase the scalability, flexibility and availability of e-learning systems. The authors have evaluated the traditional e-learning networking model, with its advances and issues, and the possibility to move the e-learning system out of schools or enterprises, inside a cloud computing infrastructure. The separation of entity roles and cost effectiveness can be considered important advantages. The institutions will be responsible for the education process, content management and delivery, and the vendor takes care of system construction, maintenance, development and management. The e-learning system can be scaled, both horizontally and vertically, and the educational organization is charged according to the number of used servers that depends on the number of students as shown in Fig.2.

The e-learning cannot completely replace teachers; it is only an updating for technology, concepts and tools, giving new content, concepts and methods for education, so the roles of teachers cannot be replaced [20]. The teachers will still play leading roles and participate in developing and making use of e-learning cloud. The blended learning strategy should improve the educational act. Moreover, the interactive content and virtual collaboration [13] guarantee a high retention factor. On the other hand, e-learning cloud is a migration of cloud computing technology in the field of e-learning, which is a future e-learning infrastructure, including all the necessary hardware and software computing resources engaging in e-learning. After these computing resources are virtualized, they can be afforded in the form of services for educational institutions, students and businesses to rent computing resources. The proposed e- learning cloud architecture can be divided into the following layers: Infrastructure layer as a dynamic and scalable physical host pool, software resource layer that offers a unified interface for e-learning developers, resource management layer that achieves loose coupling of software and hardware resources.

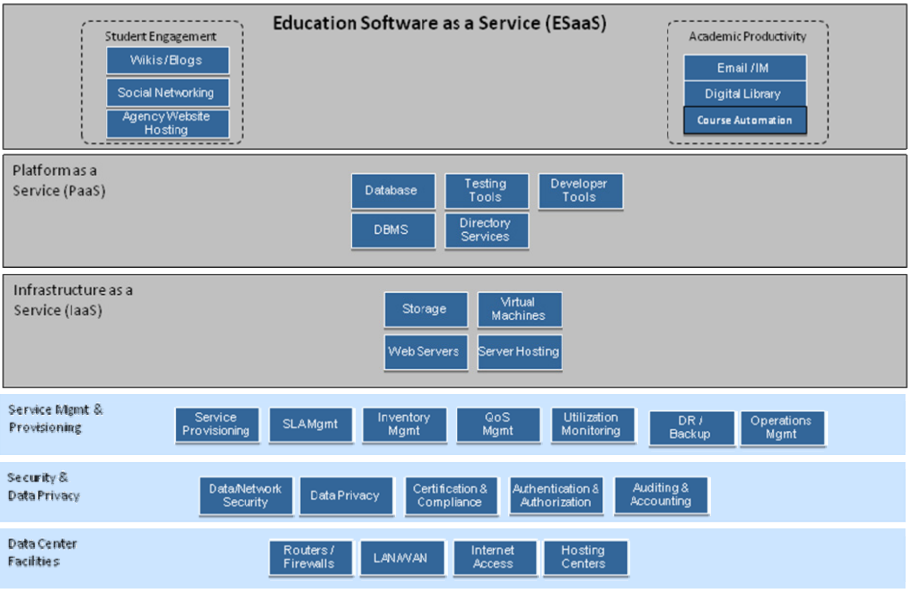

Fig. 2. Architecture for Cloud Based Higher Education System

Infrastructure layer is composed of information infrastructure and teaching resources. Information infrastructure contains Internet/Intranet, system software, information management system and some common software and hardware; teaching resources is accumulated mainly in traditional teaching model and distributed in different departments and domain. This layer is located in the lowest level of cloud service middleware, the basic computing power like physical memory, CPU, memory is provided by the layer. Through the use of virtualization technology, physical server, storage and network form virtualization group for being called by upper software platform. The physical host pool is dynamic and scalable, new physical host can be added in order to enhance physical computing power for cloud middleware services [14].

Software resource layer mainly is composed by operating system and middleware. Through middleware technology, a variety of software resources are integrated to provide a unified interface for software developers, so they can easily develop a lot of applications based on software resources and embed them in the cloud, making them available for cloud computing users. In ESaaS, cloud computing service is provided to customers. As is different from traditional software, users use software via the Internet, not need a one-time purchase for software and hardware, and not need to maintain and upgrade, simply paying a monthly fee.

Resource management layer is the key to achieve loose coupling of software resources and hardware resources. Through integration of virtualization and cloud computing scheduling strategy, on-demand free flow and distribution of software over various hardware resources can be achieved. This layer mainly consists of content production, educational objectives, content delivery technology, assessment and management component [15].

3 Privacy and Security in E-Learning

Security and privacy problems appear in e-learning because of operation mechanism and policy mechanism. The failure of security technology makes personal privacy be spread, diffused, aggrieved and scouted without permission. The primary concern in e-learning is the security that can be summarized as follows [18]:

3.1 User Authorization and Authentication

The elementary feature of e-learning system is the reliable identification – recognition of the user as a genuine member of a user community because it is the basis for Access control to the e-learning system.

Authentication – verification of the user's identity.
Authorization – permission to access specific resources. The Authorization is usually is granted only to registered students and even their access is generally restricted to a certain subset of the e-learning material based on the billing, if e-learning is offered on billing basis and on the level of learning of the registered student which will allow him/her to either to move to the next level or have a revision of the previous session.

3.2 Entry Points

There are many "entry points" in e-learning system. A system can be attacked only through its "entry points". Designers can limit the security risks by reducing the number of entry points but E-Learning system cannot be implemented using this since there are a large number of multiple users from different geographic locations.

3.3 Dynamic Nature

The other challenge is the dynamic nature of these systems where any process may join or leave the group sessions at any time. Security is also concern with each particular member process, a strict session has to be maintained and the credentials are to be verified to control both at the session level and at the participant site.

3.4 Protection against Manipulation

One of the issues of e-learning is manipulation from the side of the students the system must be secured against manipulation. There are many possible solutions where any manipulations can be protected by using the techniques of encryption, digital signatures, firewalls, etc.

3.5 Confidentiality

Confidentiality refers to the assurance that information and data are kept secret and private and are not disclosed to unauthorized persons, processes or devices. In an e-learning perspective, students need the assurance that their assignments they submit online are kept private and only disclosed to the intended examiner.

3.6 Integrity

Integrity is that only authorized users are allowed to modify the contents which include creating, changing, appending and deleting data and metadata and the attacks on integrity are generally the attempts made to actively modify or destroy information in the e- learning site without proper authorization.

3.7 Availability

The e-learning material e-content, data (or metadata) are to be made available to the learner at the specified session when the user log on to the system for their session at the period of time, if the required material is not available the learner will lose interest and not get the at most use of e-learning system. Mainly there are two types of attacks, (i) blocking attack and (ii) flooding attack, e.g.: Denial of Service, Node attacks, Line attacks, Network infrastructure attacks[16].

3.8 Non-repudiation

Non-repudiation is another important step in information security where the learners have to be provided with E-Learning services without any possible fraud such as when computer systems are broken in to or infected with Trojan horses or viruses, to deny the works or changes done by them in the system elimination of a refuted activity performed by a user.

4 Security Concerns of Cloud Computing

Security is one of the people's peak concerns on all grounds. People are more concerned of the security especially when using the technologies that involve internet. Because the internet has many loopholes that can crash the application or hack the application to gain access to the users or company details by hackers worldwide. E-learning technology is now incorporated with many latest technologies to provide more provision and reduce the complexity from traditional e-learning methodology to their users. So there is a question raised on how the cloud provides security in e-learning technology and to the e-learners. So our research throws light to identify the security issues with cloud based e-learning and the countermeasures took recently on those problems.

The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. Due to the extensive complexity of the cloud, we contend that it will be difficult to provide a holistic solution to securing the cloud, at present. Cloud system will: (i) support efficient storage of encrypted sensitive data. (ii) Store, manage and query massive amounts of data. (iii) Support fine-grained access control and (iv) support strong authentication. Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

5 Cloud Computing Based Possible Attacks

As more educational institutes move to cloud computing, more attack vectors criminals may attempt include:

Denial of Service (DoS) Attacks: Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. Twitter suffered a devastating DoS attack during 2009.

Cloud Malware Injection Attack: A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system [5]. Such kind of Cloud malware could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings. This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system.

Side Channel Attacks: An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

Authentication Attacks: Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers. Currently, regarding the architecture of SaaS, IaaS, and Paas, there is only IaaS offering this kind of information protection and data encryption.

6 Proposed Identity Authentication in Cloud Based E-Learning

Traditionally, identity authentication is applied when an individual requests access to system. For this situation, the three elements or items used for identity authentication are what you have, what you know, and what you are. Cloud computing introduces a whole new challenge for identity authentication. For an identity authentication example, consider that when a program running within the cloud needs to access some data stored in the cloud, i.e., what you have and what you are criteria are irrelevant. However, the context of the access request is relevant and can be used [18]. Only some access key and the careful monitoring protects against unauthorized access. In cloud computing (as well as other systems), there are many possible layers of access control. For example, access to the cloud, access to servers, access to services, access to databases (direct and queries via web services), access to VMs, and access to objects within a VM. Depending on the deployment model used, some of these will be controlled by the provider and others by the consumer.

Google Apps, a representative SaaS Cloud controls authentication and access to its applications, but users themselves can control access to their documents through the provided interface to the access control mechanism. In IaaS type approaches, the user can create accounts on its virtual machines and create access control lists for these users for services located on the VM. Regardless of the deployment model, the provider needs to manage the user authentication and access control procedures (to the cloud). While some providers allow federated authentication – enabling the consumer-side to manage its users, the access control management burden still lies with the provider. This requires the user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies. This can be burdensome when numerous users from different organizations with different access control policies, are involved. This proposal focuses on access control to the cloud. However, the concepts here could be applied to access control at any level, if deemed necessary. We propose a way for the consumer to manage the access control decision-making process to retain some control, requiring less trust of the provider as illustrated in Fig-3.

This approach requires the client and provider to have a pre-existing trust relationship, as well as a pre-negotiated standard way of describing resources, users, and access decisions between the cloud provider and consumer. It also needs to be able to guarantee that the provider will uphold the consumer-side's access decisions [20]. Furthermore, we need to show that this approach is at least as secure as the traditional access control model. This approach requires the data owner to be involved in all requests. Therefore, frequent access scenarios should not use this method if traffic is a concern. However, many secure data outsourcing schemes require the user to grant keys/certificates to the query side, so that every time the user queries a database, the owner needs to be involved.

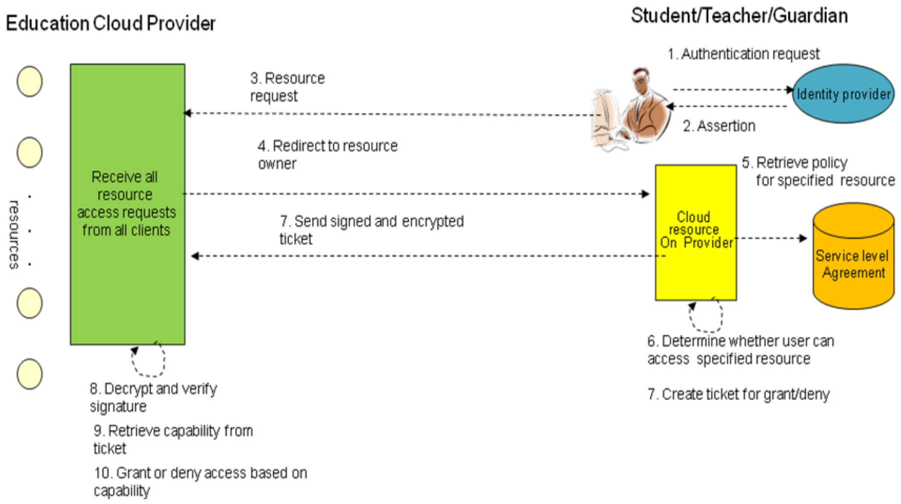
Education Cloud Provider
Student/Teacher/Guardian
1. Authentication request
Identity provider
2. Assertion
3. Resource request
4. Redirect to resource owner
5. Retrieve policy for specified resource
Receive all resource access requests from all clients
resources
7. Send signed and encrypted ticket
Cloud resource On Provider
Service level Agreement
6. Determine whether user can access specified resource
7. Create ticket for grant/deny
8. Decrypt and verify signature
9. Retrieve capability from ticket
10. Grant or deny access based on capability

Fig. 3. Proposed Identity Authentication in cloud based e-learning

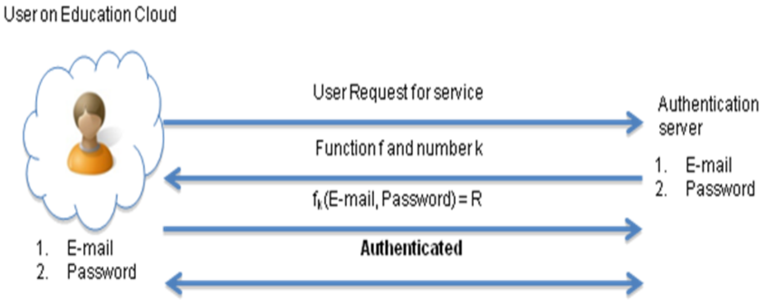

Fig. 4. Proposed Identity Authentication for proofing in details

The proposed method has the ability to use identity data on untrusted hosts i.e Self Integrity Check. It should be independent of third party. It establishes the trust of users through putting the user in control of who has his data. Identity is being used in the process of authentication, negotiation, and data exchange as in Fig. 4.

7 Conclusion

Computer security issues exacerbate with growth of Internet as more people and computers join the web, opening new ways to compromise an ever increasing amount of information and potential for damages. However, an even bigger challenge to information security has been created with the implementation of cloud computing. This paper gave a brief general description of cloud based e-learning security issues and possible directions of solutions. Some information security challenges that are specific to cloud computing have been described. Security solutions must make a trade-off between the amount of security and the level of performance cost.

Cloud computing has a dynamic nature that is flexible, scalable and multi-shared with high capacity that gives an innovative shape for e-learning systems. On the other hand, several deadly threats are affecting these benefits in cloud based e-learning systems. This research paper has discussed the influence of cloud computing in e-learning systems and the various security issues threatening the cloud based e-learning with the few guidelines to effectively handle these security issues.

The key thesis of this paper is that security solutions applied to cloud computing must span multiple levels and across functions. Our goal is spur further discussion on the evolving usage models for cloud computing and the increasing security cover these will need to address both the real and perceived issues, thus spurring new research in this area. Economic benefit of such research and resulting solutions will be increased trust in, and accelerated adoption of, cloud computing.

References

1. Masud, M. A.H., Huang, X.: ESaaS: A New Education Software Model in E-learning Systems. In: Zhu, M. (ed.) ICCIC 2011, Part V. CCIS, vol. 235, pp. 468–475. Springer, Heidelberg (2011)
2. Ahmed, S., Buragga, K., Ramani, A.K.: Security issues concern for E-Learning by Saudi universities, pp. 1579–1582. IEEE (2011)
3. Anwar, H.M., Huang, X.: Enhanced M-Learning with Cloud Computing: The Bangladesh Case. In: Proceedings of the 2011 15th International Conference on Computer Supported Cooperative Work in Design, IEEE CSCWD, Switzerland, pp. 735–741 (2011)
4. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., et al.: A View of Cloud Computing. ACM Communications 53, 50–58 (2010)
5. Viswanath, D.K., Kusuma, S., Gupta, S.K.: Cloud Computing Issues and Benefits Modern Education. Global Journal of Computer Science and Technology Cloud & Distributed, Version 1.0 12(10), 15–19 (2012)
6. Al-Rwais, S., Al-Muhtadi, J.: A Context-aware Access Control Model for Pervasive Environments. IETE Technical Review 27, 371–379 (2010)
7. Sehgal, N.K., Sohoni, S., Xiong, Y., Fritz, D., Mulia, W., Acken, J.M.: A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing. IETE Tech. Rev. 28, 279–291 (2011)
8. Anwar, H.M., Huang, X.: An E-learning System Architecture based on Cloud Computing. World Academy of Science, Engineering and Technology 62 (2012), http://www.waset.org/journals/waset/v62/v62-15.pdf

9. Zhong-ping, Z., Hui-cheng, L.: The Development and Exploring of E-Learning System on Campus Network. Journal of Shanxi Teacher's University (Natural Science Edition) 18(1), 36–40 (2004)
10. Jian, T., Lijian, F., Tao, G.: Cloud computing-based Design of Network Teaching System. Journal of TaiYuan Urban Vocational College, 159–160 (March 2010)
11. Xin-ping, H., Zhi-mei, Z., Jian, D.: Medical Informatization Based on Cloud Computing Concepts and Techniques. Journal of Medical Informatics 31(3), 6–9 (2010)
12. Méndez, J.A., González, E.J.: Implementing Motivational Features in Reactive Blended Learning: Application to an Introductory Control Engineering Course. IEEE Transactions on Education PP(99) (2011)
13. Buyya, R., Yeo, C.S., Venugopal, S.: Market-oriented Cloud computing: Vision, hype, and reality of delivering IT services as computing utilities. In: 10th IEEE Int. Conf. High Performance Comput. Comm., pp. 5–13 (2009)
14. Lijun, M., Chan, W.K., Tse, T.H.: A tale of Clouds: Paradigm comparisons and some thoughts on research issues. In: IEEE Asia-pasific Services Comput. Conf., APSCCA 2008, pp. 464–469 (2008)
15. Praveena, K., Betsy, T.: Application of Cloud Computing in Academia. Iup J. Syst. Management 7(3), 50–54 (2009)
16. Delic, K.A., Riley, J.A.: Enterprise Knowledge Clouds, Next Generation Km Syst. In: Int. Conf. Inform. Process, Knowledge Management, Cancun, Mexico, pp. 49–53 (2009)
17. Chandran, D., Kempegowda, S.: Hybrid E-learning Platform based on Cloud Architecture Model: A Proposal. In: Proc. International Conference on Signal and Image Processing (ICSIP), pp. 534–537 (2010)
18. Méndez, J.A., González, E.J.: Implementing Motivational Features in Reactive Blended Learning: Application to an Introductory Control Engineering Course. IEEE Transactions on Education (99) (2011)
19. Ouf, S., Nasr, M., Helmy, Y.: An Enhanced E-Learning Ecosystem Based on an Integration between Cloud Computing and Web2.0. In: Proc. IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), pp. 48–55 (2011)
20. Anwar, H.M., Huang, X.: A Novel Approach for Adopting Cloud-based E-learning System. In: IEEE/ACIS 11th International Conference on Computer and Information Science, China, pp. 37–42 (2012)