International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Novel Approach for Combating Cyber-Security Issues in Cloud Based E-Learning in Kenyan Universities

Judith Chepkemoi Boit[1], Watson Musyoki Kanuku[2]

Department of Computing, School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Abstract: ***Cloud based E-Learning is one of the booming technologies in Information Technology which brings powerful E-learning products with the help of cloud power. In recent years e-learning has grown into a widely accepted way of learning, and the usage of the global network is inevitable in every education process. Ubiquitous learning integrates wireless, mobile and context awareness technologies in order to detect the situation of the learners and provide more seamless adaptive support beyond formal learning process. In order to support modern pedagogical approaches, as well as a variety of heterogenic learning resources within courses, ubiquitous learning environments need to be based on a powerful IT infrastructure. At the same time, in order to be efficient, ubiquitous learning environments need to be based on learning management systems and integrated into an existing e-learning environment of educational institutions. Cloud technology has numerous advantages over the existing traditional E-Learning systems but at the same time, security is a major concern in cloud based e-learning. So security measures are unavoidable to prevent the breach of confidentiality, integrity and availability of information. Cloud based e-learning providers also need to satisfy the security needs of their customers and overcome various security threats which attack valuable data stored in cloud servers. So the survey investigated various security issues involved in cloud based e-learning technology with an aim to suggest solutions in the form of security measures and security management standards. These will help to overcome the security threats in cloud based e-learning technology.***

Keywords: E-Learning System, Learning Management System, Kenya's education sector

1. Introduction

Education has beenrecognized from time immemorial to be the bedrockfor national development. Against the milieu of unprecedented demand for formal education in in Kenya, it has become evident that the present educational model is inappropriate to meet the challenges confronting the populace. The tripartite problem of access, equity and equalityin the education sector remains a challenge. In Kenya, many qualified applicants seeking admission into mainstream institutions are being denied access to university education due to the limited physical infrastructure and other logistics existing at the universities.

Kenyan Universities are increasingly turning to e-learning as a tool to facilitate improved education. They also want to rope in more students through better access to facilities, hoping to reach a wider base in a cost-effective way.The efficiency accruing from e-learning is among the advantages gained by local universities that have adopted the use of technology and thus using different platforms, students are able follow lectures online, interact with lecturers, submit assignments and check on their grades.Lecturers are also able to upload course materials, post assignments and generate discussions online using blogs.

2. Knowledge on cyber security on Cloud based e-learning

Cloud based e-learning is the sub division of cloud computing on educational field for e-learning systems. It is the future for e-learning technology and its infrastructure. Cloud based e-learning has all the provisions like hardware and software resources to enhance the traditional e-learning infrastructure. Once the educational materials for e-learning systems are virtualized in cloud servers these materials are available for use to users and other educational businesses in the form of rent base from cloud vendors. Traditionally, identity authentication is applied when an individual requests access to a 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 the example of an identity authentication, 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. However, the context of the access request is relevant and can be used. 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, 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. All this happens as a result of virtualization. Virtualization is one of the key technologies for cloud service infrastructure. Assurance of customer Security on virtual machines is usually a daunting task and thus advanced security technologies are employed to secure them. In a typical cloud services platform, the resources provided to the users are virtual and rented in that, virtual resources and physical resources are bounded, according to the actually needs of the user. In cloud computing, multiple users share many resources, so multiple virtual resources are likely to be bound to the same physical resources. If there exists a security breach in the cloud platform virtualization software, then the user's data can be accessed by other users.

Not surprisingly, the most obvious way to attack a virtualized data center or cloud is to gain access to the hypervisor, which controls all the Virtual Machines running in the data center or cloud. For the native virtualization architecture, there have been no known attacks on a hypervisor due to its nature of being embedded in the hardware. Otherwise, two types of attacks on the hypervisor exist: attack on hypervisor through the host OS and attack on hypervisor through a guest OS.

A. Attacks on hypervisor through host Operating System(OS) is to exploit vulnerabilities of the host OS on which the hypervisor runs (Murphy 07). Due to native virtualization architecture requires specially configured hardware, most virtualization deployments are done with the hosted architecture. With vulnerabilities and security holes in most modern OSs, attacks can be done to gain control of the host OS. Since the hypervisor is simply a layer running on top of the host OS, once the attacker has control of the host OS, the hypervisor is essentially compromised. Thus, the administrative privileges of the hypervisor will enable the attacker to perform any malicious activities on any of the Virtual Machines hosted by the hypervisor. This propagation of attacks from the hosted OS to the hypervisor then to the Virtual Machines is shown in Figure 3.

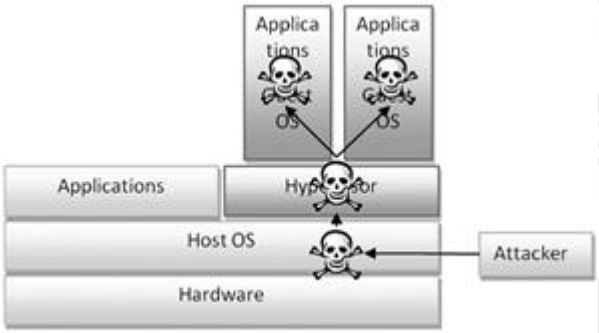

Figure 1: Attack on Hypervisor through Host OS

B. Attacks on hypervisor through guest OS is to use a guest OS to gain unauthorized access to other Virtual Machines or the hypervisor. This is also known as Virtual Machines escapes or jailbreak attacks as the attacker essentially "escapes" the confinement of the Virtual Machines into layers that are otherwise unknown to the Virtual Machine (Murphy 07). This is the most plausible attack on the hypervisor, since usually an attacker can only compromise a Virtual Machine remotely as the underlying host OS is invisible. However, since many Virtual Machine share the same physical resources, if the attacker can find how his Virtual Machines virtual resources map to the physical resources, he will be able to conduct attacks directly on the real physical resources. By modifying his virtual memory in a way that exploits how the physical resources are mapped to each Virtual Machines, the attacker can affect all the Virtual Machines, the hypervisor, and potentially other programs on that machine. Figure 4 shows the relationship between the virtual resources and the physical resources, and how the attacker can attack the hypervisor and other Virtual Machines.

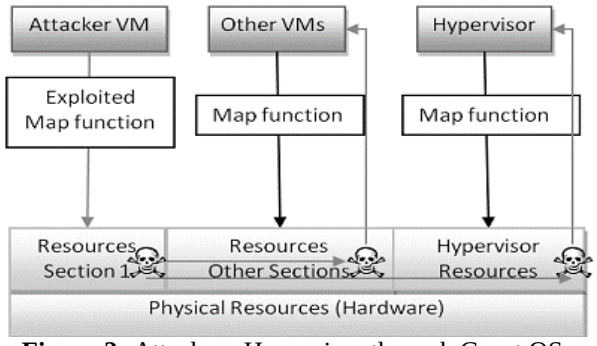

Figure 2: Attack on Hypervisor through Guest OS

3. Security Requirements

The fundamental factor defining the success of any new computing technology is the level of security it provides. Security and privacy problems appear in e-learning because of the operation mechanism and policy mechanism. The failure of security technology makes personal privacy be spread, diffused, aggrieved and scouted without permission. The following elementary security aspects should be obeyed for any kind of e-learning platforms: confidentiality, integrity, authenticity (CIA), access control, availability, nonrepudiation. A protected authentication is obligatory to recognize the user who will use the web application and to control his access privileges. This method prevents the attackers frombreaching other user's accounts accessing sensitive information or performing unauthorized processes.

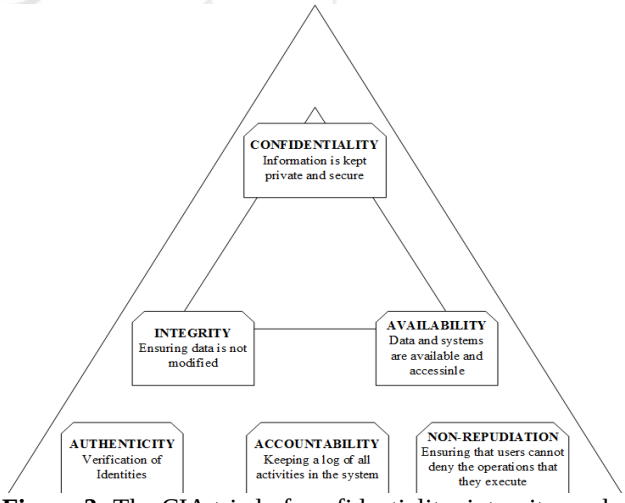

Figure 3: The CIA triad of confidentiality, integrity, and availability

The primary concern in e-learning in Kenya is the security that can be summarized as follows:

A. 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. From an eLearning perspective, students need the assurance that their assignments they submit online are kept private and only disclosed to the intended examiner.

B. Integrity

Integrity is that only authorized users are allowed to modify the contents which include creating, changing, appending

and deleting data and metadata. The attacks on integrity are generally the attempts made to actively modify or destroy information in the e-learning site without proper authorization.

C. Availability
The e-learning material, e-content, and data (or metadata) are to be made available to the learners at the specified sessions when the users log on to the system for their session at the period of time, if the required material is not available the learners will lose their interests and not get the most use of the e-learning system. Mainly there are two types of attacks; blocking attack and flooding attack, e.g. Denial of Service, Node attacks, Line attacks, and Network infrastructure attacks

D. Protection against Manipulation
One of the issues of e-learning is the manipulation from the side of the students. The system must be secured against manipulation. There are many possible solutions in which any manipulations can be protected by using the techniques of encryption, digital signatures, and firewalls.

E. User Authorization and Authentication
The elementary feature of an e-learning system is the reliable identification – recognition of a 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 granted only to registered students and even their access are generally restricted to the appropriate part of e-learning materials based on the billing. If e-learning is offered on the billing basis and on the level of learning of the registered student, this will allow him/her to either to move to the next level or have a revision of the previous session.

F. Entry Points
There are many "entry points" in an 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 systems cannot be implemented using this since there are a large number of multiple users from different geographic locations.

G. Dynamic Nature
The other challenge is the dynamic nature of e-learning systems where any process may join or leave the group sessions at any time. Security is also concerned 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.

H. 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. For example, 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. The Solution for Kenyan Universities

This proposed model seeks to guide universities within the Kenya's education sector on their bid to securely implement Cloud Based eLearning and seeks to inform on the various security threats and challenges associated. This model seeks to address the convergence of concepts from different technologies in advocating for an effective methodology for implementing Cloud Based eLearning in the various deployment techniques that is Public, Private and Hybrid. Emergence of cloud computing owes significantly to mash-up. Based on this idea, various security architectures such as: a secure component model addressing the problem of securing mash-up applications and an entropy based security framework for cloud oriented service mash-ups have been proposed in. Also, privacy needs to be maintained as there are high chances of an eavesdropper beingable to sneak in.This diagram provides a cloud based model to secure E-Learning Environment. The E-Learning users, Secured Layer and 3rd party providers are taken into consideration in the design of this model. The cloud based model to secure E-Learning environment is shown in Figure 3.

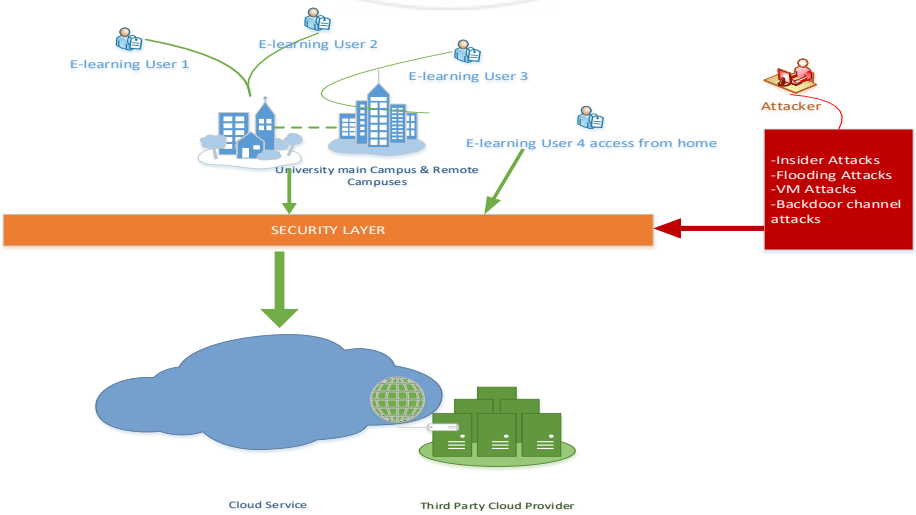

Figure 4: Model for Cloud Based E-learning security

The solutions provided by the model seeks to describe the security layer enforced on Cloud Based E-learning based on virtualization architecture and aims to solve security vulnerabilities by employing security measures on the virtualization components and characteristics. The three major approaches employed in this model are hypervisor security, guest OS security, and image management security.

1) **Hypervisor security** is the application of traditional security measures to the hypervisor. This is a principle component of virtualization security. The hypervisor is the entire management layer for a virtualized system. Thus, if the hypervisor is compromised, then so are all the Virtual Machines created or controlled by the hypervisor. As long as the security of the hypervisor is strong enough, compromising all the Virtual Machines will be difficult for the attacker. For native virtualization architecture, there are currently many physical ways to ensure access control to the hypervisor. An example would be a hardware token possessed by the administrator in order to launch the hypervisor. However, as noted before, attacks on hypervisor in a native virtualization architecture is currently not known, thus making hypervisor security on such architecture almost irrelevant. For hosted virtualization architecture, traditional ways to protect running processes on an OS are currently implemented to protect the hypervisor. Security measures such as access control, automatic updating, networking, and introspection on guest OSs are all ways to protect the hypervisor from unauthorized access. These elements of security are generally implemented in software and can be easily updated to keep the security features of the hypervisor up to date.
2) **Guest OS security** is the application of traditional security measures to the guest OSs . This may sound like a redundant process to hypervisor security, but in virtualization, every component must be secure in order for the virtualized system to be secure. Since guest OSs running on a Virtual Machines behave just like a real OS on physical machine, important security measures for single instance OSs are deployed on each guest OS. Also, each guest OS must have sufficient isolation so one Virtual Machine being compromised does not lead to other Virtual Machines on the same machine being compromised. More importantly, since guest OSs can use physical peripherals available on the machine, the communication between guest OSs and the hypervisor must be secure and the abstraction provided by the hypervisor must be enforced. Currently, many virtualization security firms are using guest OS monitoring to detect and quarantine infected guest OSs or revert them to a previous stage with stored guest OS images.
3) **Image management security** is the securing of how Virtual Machine images are stored, transported, and managed in a virtualized data center or cloud. This is an important aspect of security in virtualization due to mobility and variable state in each Virtual Machines, and how attackers exploit the fact that security measures are weaker on the network or backup data centers. Thus, to achieve image management security, strong storage encryption must be applied so sensitive data does not leak from the images; strong network security must be in place to ensure safe transportation of Virtual Machine images. Another fact to consider is that Virtual Machine images can be created quickly and easily. This can generate many unnecessary distributions of the same Virtual Machine, and this vulnerability is generally called Virtual Machinesprawl. In order to control the unnecessary distribution of Virtual Machine images, a strong access control on the image management facility must be in place. Virtual Machine software companies generally implement different levels of authority to control how each image can be managed to ensure image management security. The solutions discussed above are all generic approaches to achieving security in virtualization. The actual implementations of these approaches can differ significantly, and it is outside the scope of this paper to discuss them. In addition to securing the components in virtualization, security measures in the infrastructure itself can greatly reduce the possibility of attacks.

The solutions based on virtualization infrastructure aims to solve security vulnerabilities by creating secure gateways in the virtualization infrastructure. This set of solution is predominantly for data centers and clouds as infrastructure is an integral part in the construction process. The two dominant areas are security on the virtual layer and security on the physical layer.

1) **Security on virtual layer** is achieved by securing how Virtual Machines and hypervisors talk to each other in a virtual network. In order to take full advantage of the virtualization infrastructure, virtual private networks (VPNs) are commonly created to manage different levels of authority in Virtual Machines. Because of the virtual nature of the network, features such as monitoring, access controls, integrity, encryption, authentication, and transportability of Virtual Machines can be implemented directly into the network. This will solve many of the vulnerabilities present in a virtualization as the security on the virtual layer will isolate different virtual management networks and bring ease to deployment and operation of Virtual Machines across different authorities or data centers.
2) **Security on physical layer** is the design of the structure of the physical systems that brings about security in a virtualized environment. One of the most notable features in this area is host-based intrusion detection and prevention (Randell 06). It allows the system to ensure that at least the physical layer will not be compromised easily through other means. The structure of the data center or the cloud also plays an important role. How the machines that are running the VMs interconnected physically can determine the possible security measures that can be used. Also, routine inspection for hardware failures and outdated systems is part of the security on the physical infrastructure that plays a large role in determining how secure the virtualized environment is.

Although it is outside the scope of this thesis to discuss how each solution is implemented this model tends to summarize the solution as a product for offering security in Cloud Based eLearning.

Based on infrastructure of virtualization I do believe that malware can enter from various levels of the virtualization

infrastructure such as apps running on the guest Operating Systems, apps on the host Operating Systems, or even the Operating Systems themselves (Trend 2009). Therefore, I deployed various levels of security on the virtual security layer to protect the entire system. For example, the solution consists of a watch dog on the hypervisor level that solves the issues of monitoring and attacks on the hypervisor from the host Operating System. The solution also consists of intrusion detection modules on each of the Virtual Machines. This will solve the vulnerability issue due to concentration since each Virtual Machine has its own self defense mechanisms from the hypervisor. The infrastructure of the solution is shown in Figure 5. The security components are shaded in green.

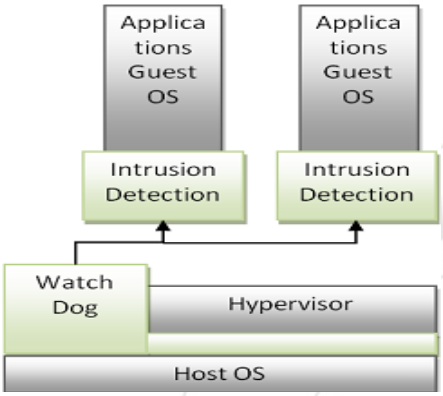

Figure 5: Virtualization Security on applications and operating systems

The other way this model solves the problem is by combining the security on the virtual layer and physical layer. The intention is that it would be easy for Institution to set up an already secured virtualization infrastructure. In each physical layer institutions can integrate their own hardware security features for example with Cisco's networking equipment, and on top of that, the Virtual Machine ware is integrated as part of the physical block. Because of the heavy integration between the physical layer, the networking layer, and the virtual layer, and each having their own sets of security and defense mechanisms, security comes as a pre-integrated and secure infrastructure for any data center or cloud to use. This implementation solves the internal vulnerabilities that most Learning institutions face since most already have a strong perimeter defense against intrusions. The infrastructure of security in a virtualized environment is shown in Figure 6.

Virtual Block

Virtual Applications		
Virtual Machine ware	Virtual Machine ware	Virtual Machine ware
Cisco	Cisco	Cisco
Hardware	Hardware	Hardware

Figure 6: Infrastructure with Virtual block

5. Conclusion

This paper shows several security aspects of e-learning platforms in general and mainly, we examined the most significant concerns of the famous open source learning system, Moodle. The development of the e-learning systems should be created by applying secure functions and internationally recognized standards. The development requires that security services (e.g. authentication), encryption, access control, managing users and their permissions to be implemented. The data transfer between the system and administrators or content operators should be implemented on encrypted SSL channels via the web administration interface. A secure learning platform must integrate all aspects of security and secure mechanism without influencing the system performance a lot.

References

[1] AHMED, S., BURAGGA, K. & RAMANI, A. K. Year. Security issues concern for E-Learning by Saudi universities. *In*, 2011. IEEE, 1579-1582.

[2] AL-JUMEILY, D., WILLIAMS, D., HUSSAIN, A. & GRIFFITHS, P. 2010. Can We Truly Learn from A Cloud Or Is It Just A Lot of Thunder? *2010 Developments in E-systems Engineering*, 131-139.

[3] ANGEL_LEARNING. 2011. *Application Hosting Services* [Online]. Available: http://www.angellearning.com/services/application_hosting.html [Accessed July 25 2011].

[4] ANGEL_LEARNING. 2011. *Standards Leadership* [Online]. Available: http://www.angellearning.com/products/lms/standards.html [Accessed July 25 2011].

[5] ANGEL_LEARNING. 2011. *Technology and Systems Integration* [Online]. Available: http://www.angellearning.com/products/lms/tech_systems.html [Accessed July 25 2011].

[6] BENEDIKTSSON, D. 1989. Hermeneutics: Dimensions toward LIS Thinking. *Library and information science research*, 11, 201-34.

[7] BLACKBOARD. 2011. *About Bb* [Online]. Available: http://www.blackboard.com/About-Bb/Company.aspx [Accessed July 25 2011].

[8] BLACKBOARD. 2011. *Association Clients* [Online]. Available: http://www.blackboard.com/Markets/Associations/Clients.aspx [Accessed July 25 2011].
[9] BLUMBERG, B., COOPER, D. R. & SCHINDLER, P. S. 2005. *Business research methods*, McGraw-hill education.
[10] BOEIJE, H. 2002. A purposeful approach to the constant comparative method in the analysis of qualitative interviews. *Quality and Quantity*, 36, 391-409.
[11] BOTT, E. 2011. *Google's Blogger outage makes the case against a cloud-only strategy* [Online]. www.zdnet.com. Available: http://www.zdnet.com/blog/bott/googles-blogger-outage-makes-the-case-against-a-cloud-only-strategy/3300 [Accessed May 13 2011].
[12] CARLIN, S. & CURRAN, K. 2011. Cloud Computing Security. *International Journal of Ambient Computing and Intelligence*, 3.
[13] CASQUERO, O., PORTILLO, J., OVELAR, R., ROMO, J. & BENITO, M. 2010. Strategy approach for eLearning 2.0 deployment in Universities. *Digital Education Review*, 1-8.
[14] CHISNALL, P. M. 1981. *Marketing research: analysis and measurement*, McGraw-Hill London.
[15] CHOW, R., GOLLE, P., JAKOBSSON, M., SHI, E., STADDON, J., MASUOKA, R. & MOLINA, J. Year. Controlling data in the cloud: outsourcing computation without outsourcing control. *In*, 2009. ACM, 85-90. 63
[16] COOPER, D. R., SCHINDLER, P. S. & SUN, J. 1998. *Business research methods*, Irwin/McGraw-Hill Burr Ridge, IL.
[17] DHILLON, G. & BACKHOUSE, J. 2000. Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43, 125-128.
[18] DOCEBO. 2011. *Docebo E-Learning solutions* [Online]. Available: http://www.docebo.com/cms/home_elearning_lms_multimeda_courses [Accessed July 25 2011].
[19] DOCEBO. 2011. *DoceboLMS E-Learning Platform* [Online]. Available: http://www.docebo.com/cms/page/61/Docebo_LMS_learning_system [Accessed July 25 2011].
[20] DOCEBO. 2011. *DoceboLMS Features* [Online]. Available: http://www.docebo.com/files/brochure/DoceboLMS_Features_ENG.xls [Accessed July 25 2011].
[21] DOCEBO. 2011. *E-Learning solutions overview* [Online]. Available: http://www.docebo.com/cms/page/59/Elearn_and_Online_learning_solutions [Accessed July 25 2011].
[22] DOCEBO. 2011. *Why choose DoceboLMS?* [Online]. Available: http://www.docebo.com/community/doceboCms/set-language_English_language-english.html [Accessed July 25 2011].
[23] DOWNES, S. 2006. E-learning 2.0. *eLearning magazine: education and technology in perspective', http://elearnmag. org/subpage. cfm*, 29-1.
[24] EAVES, M., MACLEAN, H., HEPPELL, S., PICKERING, S., POPAT, K. & BLANC, A. 2007. Virtually There: Learning Platforms. Scunthorpe: Yorkshire and Humber Grid for Learning Foundation/Chelmsford: Cleveratom.
[25] EL-KHATIB, K., KORBA, L., XU, Y. & YEE, G. 2003. Privacy and security in e-learning. *International Journal of Distance Education Technologies*, 1, 1-19.
[26] FOSTER, I., ZHAO, Y., RAICU, I. & LU, S. Year. Cloud computing and grid computing 360-degree compared. *In*, 2008. Ieee, 1-10.
[27] GAMMACK, J., HOBBS, V. & PIGOTT, D. 2006. *The book of informatics*, Nelson Australia.
[28] HOLLISTER, S. 2011. *Gmail accidentally resetting accounts, years of correspondence vanish into the cloud?* [Online]. www.zdnet.com. Available: http://www.engadget.com/2011/02/27/gmail-accidentally-resetting-accounts-years-of-correspondence-v/ [Accessed Feb 27 2011].
[29] HU, Z. & ZHANG, S. Year. Blended/hybrid course design in Active Learning Cloud at South Dakota State University. *In*, 2010. IEEE, V1-63-V1-67.
[30] IWEBTOOL. 2011. *What is End User?* [Online]. Available: http://www.iwebtool.com/what_is_end_user.html [Accessed July 25 2011]. 64
[31] JAMIL, D. & ZAKI, H. 2011. CLOUD COMPUTING SECURITY. *International Journal of Engineering Science and Technology (IJEST)*.
[32] JENSEN, M., SCHWENK, J., GRUSCHKA, N. & IACONO, L. L. Year. On technical security issues in cloud computing. *In*, 2009. Ieee, 109-116.
[33] KUMAR, A., PAKALA, R., RAGADE, R. & WONG, J. Year. The virtual learning environment system. *In*, 1998. IEEE, 711-716 vol. 2.
[34] LAISHENG, X. & ZHENGXIA, W. Year. Cloud Computing: A New Business Paradigm for E-learning. *In*, 2011. IEEE, 716-719.
[35] LI, J. Year. Study on the Development of Mobile Learning Promoted by Cloud Computing. *In*, 2010. IEEE, 1-4.
[36] MOODLEROOMS. 2011. *About Moodlerooms*[Online]. Available: http://www.moodlerooms.com/company/about-us/ [Accessed July 25 2011].