World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:7, No:9, 2013

Cloud Computing for E-Learning with More Emphasis on Security Issues

Sajjad Hashemi, Seyyed Yasser Hashemi

***Abstract*—**In today's world, success of most systems depend on the use of new technologies and information technology (IT) which aimed to increase efficiency and satisfaction of users. One of the most important systems that use information technology to deliver services is the education system. But for educational services in the form of E-learning systems, hardware and software equipment should be containing high quality, which requires substantial investment. Because the vast majority of educational establishments can not invest in this area so the best way for them is reducing the costs and providing the E-learning services by using cloud computing. But according to the novelty of the cloud technology, it can create challenges and concerns that the most noted among them are security issues. Security concerns about cloud-based E-learning products are critical and security measures essential to protect valuable data of users from security vulnerabilities in products. Thus, the success of these products happened if customers meet security requirements then can overcome security threats. In this paper tried to explore cloud computing and its positive impact on E- learning and put main focus to identify security issues that related to cloud-based E-learning efforts which have been improve security and provide solutions in management challenges.

***Keywords*—**Cloud computing, E-Learning, Security.

I. Introduction

THE simplest definition for cloud computing, which can be expressed by users in terms of the access to new applications, is based on the tenancy [1]. In other words, cloud computing is the next generation of Internet-based distributed computing systems which have high scalability and computing resources in the 'as a service' provided [2]. Cloud computing is an important pattern, with significant potential for reducing costs through optimization and performance and increasing economic efficiency, which can significantly, increases collaboration, agility and scalability [3]. This technology provides many opportunities to large corporations and IT companies in the developed countries, but these opportunities face with challenges that cloud computing is one of the major concerns in this field [4]. If security measures are not applied correctly, all areas of cloud computing, encountered into a problem [5]. It can be state that the adoption of cloud security is a vital highway, and if the providers of this technology can minimize the major obstacle, then the use and the acceptance of Cloud IT will be easier [6]. E-learning software pointed to educational services that can be provided based on the Internet and by virtual websites. It can also be offered by the internet system and also by considering that, cloud computing is a platform as well as the Internet, therefor as a result, the system of cloud-based services can be offered. However, to maintain the cloud-based E-learning effective and successful, it needs the security of cloud-based E-learning products which should be identified and resolved. In this paper, attempts to investigate the benefits of cloud computing for E-learning with an emphasis on security issues, and based on it, tried to have successful results which is needed to secure cloud-based E-learning products, and for security of users, especially security of data and stored information in the cloud servers.

This chapter structured as an introduction of the cloud computing, security and E-learning. Section II defines cloud computing models and various characteristics of it. Section III, involves the definition of E-earning and includes issues surrounding it. Section IV as well as Section V includes the benefits of cloud computing for E-learning, including cloud-based security issues, and finally, in Section VI in this paper, conclusions and future studies are mentioned.

II. Cloud Computing

Many definitions for cloud computing have been proposed by researchers. But there is no agreement on a specific definition. America by the National Institute of Standards and Technology's definition of cloud computing is follows as below [3]-[6]. Cloud computing is a model for enabling convenient access to networks and applications, common set of configurable computing resources (eg, networks, servers, storage and applications) that can be provided and released immediately with minimal effort or involvement. The basic idea of cloud computing is making the pool of virtual computing resources with a focus on large scale computing resources that are connected to the network, and which allows customers to be shared dynamic hardware, software resources and data, and according to their actual usage, paying costs. Thus, we can buy and sell easily the cloud computing like goods through the network with a lower price, just like water, gas and electricity sold [7]. Now to recognize and accept the main features of cloud computing, we should understand developed models, and how to use the service and how to protect it [3]. Here are the five key features of cloud computing [6]-[8]:

- **Service demand on self.** By using this feature, the customer can easily and automatically access to

Sajjad Hashemi is with the Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran (e-mail: Iau.hashemi@gmail.com).

Seyyed Yasser Hashemi is with the Department of Computer Engineering, miyandoab Branch, Islamic Azad University, miyandoab, Iran (e-mail: hashemi.uni@gmail.com).

computing facilities like server, net, storage from any provider as soon as possible.

- **Ubiquitous network access.** It implies that the facilities are accessible on the net and they can be used following standard methods. The methods can support weak and strong clients like laptop and mobile phones.
- **Location-independent resource pooling.** This feature of pools for different customers needed resources in the same place dynamically by the providers. These resources can include the storage, memory, the bandwidth of net and virtual machines.
- **Rapid elasticity.** By using this feature, the facilities can be provided rapidly and with high elasticity then it can be expand or release fast. In other words the services can always be updated and improved to be accessible for the users.
- **Measured service.** This feature enables monitoring, controlling and reporting of the resources, and can apparently control and report the amount and the quantity of resources for the using of both customer and the provider of the infrastructure.

In other words all these features cover the coherence and appearance of the clouds [3].

Different cloud models are: public, private, and grouped and hybrid clouds [3]-[6]. Public clouds are available to the public and can be accessed by different tenants, where resources, applications and web services are provided over the Internet can provide the infrastructure for implementing it, helped by organizations [9]. While private cloud, is just one organization, so everyone can access within the organization, services and applications but users outside the organization cannot access into the Cloud [9]. Cloud infrastructure for an organization is used [10]. Thus, a private cloud infrastructure management keeps the organizations' information protected fully by organization [3]. Similarly, the cloud group is designed for a specific group of customers [6] and its infrastructure, shared between several organizations and a specific group supports security needs, however sharing between multi-organizations will be involved concerns [10]. Hybrid clouds, the latest model, are a combination of two or more clouds (public, private or group). In fact it is the environment in which internal and external cloud services from multiple providers are used [9].

Various services of cloud are presented into three models which are [3]-[6]: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

- **SaaS,** in this section the customer doesn't manage the infra-structure of cloud that includes the net, servers, operational systems, and saving area, except the functional software to limited the degree of adjustment at the level of user. Consequently the companies are not interested in SaaS because the security concern of companies is the main hindrance in accepting them.
- **PaaS,** in this kind of service, the client has the option for putting the purchased functional programs on the infra-structure of cloud. Here also the client dose not mange or control infrastructure of the cloud such as the net, servers, storage. He just has control the functional program that installed or Settled by him. In fact the PaaS is similar to SaaS; the only difference is that PaaS includes exclusive program environment and computing platform, for developing and solution strategies.
- **IaaS,** The client dose not manage or control infra-structure but has control over the operational system, saving area, and the established programs. In this service an artificial server is completely available for the client.

III. E-Learning Environment

E-learning environment is an environment, in which students via E-learning applications and tools related to the subjects of study. Virtual Learning Environments and personal learning environment are the most important environments of E-learning environments that present a wide range of opportunities to students through E-learning applications in their studies [11]. The main advantage of a virtual learning environment (VLE) is storing multiple topics at the same time, which can provide a suitable environment for teachers and students to move from one topic to the next topic, in addition, VLE also provides other facilities, Such as [12]:

1) Announcements page for update information on course topics.
2) Students can take their courses in their account at any time and from any place.
3) Students allowed with special needs and limitations for this type of E-learning system.
4) Provides training in a geographically large-scale.
5) Via the internet (because of the flexibility and cost effectiveness helps students) it will facilitate learning.
6) Small schools which may not have a large selection of courses by using the VLE, more selective courses be available to students.
7) Provides possibility of interaction between students and lecturers.

Personal Learning Environment (PLE) is a single-user of E-learning system which allows students to manage and improve their learning process. PLE supports a series of features that are available for most users [11]-[13]:

1) In the E-learning system, students can improve and fix their learning goals.
2) Users can manage teaching and learning materials in E-learning systems.
3) Users in their learning process in E-learning system can communicate with other users.

Actually it should be noted that E-learning cannot fully substitute instead of teachers, in fact although the learning concepts and contents with new methods presented, however it is not possible to replace instead of the role of teachers, because teachers have the main role in development and facilitative of E-learning [4].

IV. The Benefits of Cloud-Based E-learning

Cloud-based E-learning is a part of cloud computing, which is related to the field of education and E-learning systems. Cloud-based E-learning resources traditionally included all required hardware and software infrastructure to enhance E-learning [11]. Educational issues for E-learning systems in cloud servers are virtual and the topics that used for students and their business are available based on cloud tenant from vendors [11].

1) **Virtualization:** It makes possible for the rapid replacement of a compromised cloud located server without major costs or damages. Cloud reduced substantially expected time because it is very easy to create a clone for a virtual machine [14], [15].
2) **Centralized Data Storage:** As the most important part of the applications and data are stored into the cloud, losing a cloud client is not a major incident in the cloud computing. So, new client can be connected very fast [14], [15].
3) **Benefits for students:** Many students gain benefit from cloud-based E-learning. They can take online courses, Participate in online testing, receive feedback about the teachers training, teachers and send their assignments and projects, to the online teacher [16].
4) **Benefits for Teachers:** Teachers are also gaining many benefits from cloud-based E-learning. Teachers can prepare online tests for students; they can prepare Resources for students with the best content from the CMS, can evaluate and answer assignments and projects, and can communicate online with students through the forums [11]-[16].
5) **Easy Monitoring:** Only one place should be supervised instead of monitoring thousands of computers belonging to a university, by this way, monitoring of data access becomes much easier. Also the security changes can be tested and implemented without any difficulty since the cloud represents a unique entry point for all the clients [14].
6) **Reduce costs:** users of E-learning do not require a PC with powerful hardware specifications for E-learning applications. They can deploy applications to run in the cloud from their computer, mobile phone, and tablet with internet connection with a minimum configuration. Since the data is available in the cloud and users do not need to pay a large fee to upgrade the memory to store in local machines. So organizations will be renting a space in the cloud based for their needs [17].
7) **Improve the performance:** since the applications of cloud-based E-learning are applicator programs and have many processes in the cloud, so any problem will happened when client machines are activated [18].
8) **Rapid software updates:** Since the application programs based on cloud implemented for cloud-based E –learning environment, so the software will automatically update the source cloud. Then always E-learning users get update software [11]-[18].
9) **Improved compatibility of document formats:** Because the files' formats and fonts do not proper on PCs / mobile phones therefore all formats are for the cloud with E-learning applications, so there is nothing to worry. Because cloud-based E-learning applications, open files through the cloud environment [11]-[18]

V. Security Issues in Cloud Based E-Learning

Security issues in new technologies are important because most users expect IT as a guarantee to security. Since the cloud-based E-learning is available through web-based resources so there are numerous security threats from the Internet for the cloud-based E-learning users. Although cloud for E-learning has brought many benefits, but yet uncertainties do not fully meet in cloud security and still there are the security challenges and issues in the digital world [19]. In previous years cloud service companies as well as vendors of E-learning, provide solutions as well as security measures and standards which are necessary to overcome the problems of security applications and required standards for security issues of E-learning [11]. Since each cloud computing and E-learning threated, So at first briefly some of these challenges and threats will explained and in continue security measures for cloud-based E-learning will introduced.

A. Security Threats to Cloud Computing

1) **Primary security considerations:** It is required to involve the awareness or control of running criteria over the utility of the resources as they are being shared by the customers of third party in the system. Most of the services have not the similarities in characterizations with cloud systems. Hence it is to come across a little difficulty at the time of transferring the services of utility from cloud system to other different system [19]. During the cloud services it must maintain an encryption/decryption keys by authorized users. There should be an essential step of ensuring each process of transferring, storing and retrieval of the information. And a combined method of these functions needs to be associated with certain standards [19].
2) **Availability:** Access to applications and important data on cloud servers for uninterrupted services to customers in the cloud computing is a major concern. A Denial-of-service attack (DoS Attack) or Distributed-Denial-of-service attack (DDoS Attack) are the most popular online attacks that affect the availability of online services and make the stored data inaccessible to users in the server [11].
3) **Data Lock-in:** Today, cloud providers, provide numerous tools, applications and standard data formats to their customers. But these services encounter to the problems when a client tries to use the services of another provider [11]-[19]. Because most cloud providers are not compatible with each other. So customers can not migrate to another cloud service operator. This problem provides

difficulties in getting services from cloud operators [20].

4) **Browser Security:** Cloud computing tasks related to remote servers. Machine Clients only use I / O devices to access any application. In this case, the browser on the machine client used as a gateway to access cloud servers [11]. Therefore, the security of the entire cloud browser is critical because if gateway attacked by software attackers, the overall security of the cloud will become a problem. Security policies and authentication certificates required for secure browser. XML Signature and XML Encryption also help to be ensuring of security issues [21].
5) **Insecure of Incomplete data deletion:** In most operating systems, data is not deleted completely even after the data erased from their physical machine. Customers are not able to know, whether their data is fully wiped out from all the virtual machines once after the delete command is applied. This problem leads to unsecured data on cloud. And also there may be a risk of this stolen data that used by unauthorized persons or hackers from the cloud [11]-[20].
6) **Increased Authentication demands:** Cloud providers offer various advantages to their customers, one of them is providing the software and accessing its application online. So client machine does not need to install with any software applications to access to its functionality. Users do not bother about software privacy as they are run by centralized monitoring servers through cloud. But cloud providers should be careful to provide authentication to their customers to access by authorized persons. If cloud operators fail to provide these authentication procedures, it may lead to increase the threat of phishing or other vulnerabilities through unauthorized access of those applications on cloud [11]-[22].

B. E-Learning Security Threats

Usually, basic security in E-learning technologies concerns when we used that for traditional learning applications equipment. These concerns are given below [11]-[23]:

1) **User authentication and User License:** for the user to enter in E-learning environment is an important and essential license. In general, E-learning users are in different and far from places so user ID and password should be provided. Learner or student based on the permission that defined for the account can access to the facility. Based on billing Methods he/she may allow to access to the next level of learning rules (learning provision) or not.
2) **Entry points:** the input entries, the number of terminals are passive ways in which a security breach may occur in the case of E-learning. Because the number of clients, access to E-learning servers from remote areas, then so much input entries will result in security threats.
3) **Protection against tampering:** protection against manipulation is one of the key tasks that must be implemented in an E-learning environment. It can be prevented other users by using certain techniques like digital signatures, firewalls etc. Similarly several other measures have to be taken in order to avoid manipulation from the registered users. Thus E-learning environment gets enhanced by following and using the security measures carefully which will create a smooth structure of data flow along the network.
4) **Non-Repudiation:** In this stage of information security, the format of the data is destroyed or damaged by virus, (TROJAN horses and other malicious threats are common). The system must be provide with much capability in that no data changed by the attacks.
5) **Social aspects of security:** Online E-learning environment is different from traditional learning environment. Major changes have taken place in the assignments submitted by students to teachers. In a traditional learning environment, students were provided directly their assignments in hard copy format to teachers in class rooms. While in an online E-learning environment, students need uploading a soft copy for their assignments. Therefore, this type of method in e-learning technology brings threats and vulnerabilities through the Internet for E-learning system. To overcome these problems, the basic safety requirements such as integrity, confidentiality and availability are observed.

VI. Security Measures in Cloud Based E-Learning

The main concern for the information technology especially in the field of cloud computing is security. According to an article published by the Educause ("nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology") from 2005 to 2011, the main concern of security was in the fourth issue in the field of Information Technology (IT). Security continues to be an integral component of information technology, so that in 2012 it was one of the 10 key issues related to information technology [15]. When E-learning moves to the cloud, security concerns about the reliability of the original system, confidentiality, integrity and availability will be happened.

In this section, some security measures for securing cloud-based E-learning will be introduced. As noted, the cloud-based E-learning comprised of both E-learning with cloud computing technology so both IT security measures and procedures must be consider to overcome security threats.

A. Security Measures Taken in Cloud Computing

There are varieties of security measures to overcome security threats in cloud computing, by vendors. These security measures used to overcome security problems and to answer the threats, that some of these actions are as following [15]:

1) **Software as a Service (SaaS) security:** Many security measures and practices in the SaaS which are service presentation model, are based in cloud. Before the acceptance by users of the service model or companies, they should be aware about the security of data and sell

policies. Before using their services they can block the unintended access of the data.

2) **Surveillance and security consciousness:** within the organization, security committee can be form with the purpose of providing guidance and care about the security strategies of the organization. The committee shall be clearly defines the roles and responsibilities of security functions. Also Security awareness is also an important work to be done. The lack of proper security alert, forced to disclose or disclosure of crucial data. In contrast, the organization will be vulnerable to threats. Social engineering attacks slow the respond to potential security events and can cause huge financial losses to the organization, which is a result of poor security consciousness.
3) **Education and Training:** This phase includes training on basic security issues and crisis management skills (risk), it is for the security team and local partners. It includes the introduction or definition of security and provides training and mentoring skills for team members who can serve as the basis for their Certified (Home Security Fundamental Security) which is also the name of the confidentiality of data and knowledge management.
4) **Methods and Standards:** always examining the sources and patterns to develop methods and standards for cloud computing systems is a good way. The first and the most important thing that security team should be consider is security of data with needs of business. These procedures should be provided with appropriate documentation and supporting documentation must also be defined for standard methods (they have to follow these procedures as a framework). To maintain the relationship (having continuity over time) the standards and methods have occasionally (no specific time cycle) taking into account and review the fundamental changes in the business or IT environment.

Other security measures in cloud computing are as follow which just enough to name them. Data privacy, Disaster recovery, Physical security, Change management, Identity Access Management (IAM), Virtual machine security, Application security, Data security, Data governance, Security image testing, Vulnerability assessment, Third party risk management.

B. Security Done on E-Learning

A number of anticipated have been made to overcome the security threats and potential security vulnerabilities in the cloud-based E-learning by sellers and organizations which are used technology. Apart from all these security predictions, E-learning technology is capable for some mechanisms to resolve potential vulnerabilities and other threats on the Internet to protect E-learning form the attacks. The security mechanisms are as follows [11]:

1) **Security mechanism of SMS:** This process (legally accepted) used by a legitimate user in E-learning environments. Procedure (Team Viewer) helps user to be enter in E-learning server by his/her username and password that provided during registration. After entering to an environment, each individual user will received a password via SMS on his mobile which recorded number in the system. Therefore the security is maintained. Since the phase of password codes vary from meeting to meeting, with the identified illegal entry mainly stipulated by the alien users, illegal instruction of E- learning has stopped.
2) **Biometric mechanism**: This mechanism allows legal users to use one or more physical or behavioral characteristics. During the registration phase, the user’s physical and personal characteristics such as fingerprints, iris recognition, voice recognition or behavioral traits and ... collected. This information will be stored in the database. The user's login properties with features stored in the database and will be compared by using biometric scanning devices such as the fingerprints mouse. If the content of this specification is equivalent, the content of E-learning will be provided to the user. In this process, the process requires the physical presence of a person which is very intelligent, reliable and secure.
3) **Security check:** It is a common method for license of students by many universities which provide a hardware security feature. Sometimes it is also called secret evidence. And used as a key to access E-learning system. This option is also provided with a password that by showing the electronic identity (logging) and by entering the password, user can access to a system.
4) **ACL Mechanism:** ACL or accessible control list is a process to access server or specific resource that the user can access to mechanism by customization factor. ACL coefficient attached or embedded within the file, for example, the user will be add "Shame" to have access to a system. Then the user will have defined “Shame" in ACL file for accessing to system. We also can make functions available like read, write, or delete for user. This shame option make user to access editing or removing certain files which are mechanisms based on host and all permits are approved and controlled by the Service Provider.
5) **Digital Signature:** Digital signatures are used to authenticate the identity of the sender. At first electronic signature during the sending to receiver has been created by an uncertain network. A certificate signed by the sender with a message which is a complex algorithm and a private key of the sender's computer will be present. The main advantage of digital signatures is undeniable. Although the sender claims that he did not sign the message and his private key is kept secret, so it is possible to claim that, the use of some algorithms that can make a Stamp time undeniably, received the message from sender. It is also possible to check the data that may manipulated by the user or not.
6) **Security due to passive attacks:** in all methods that mentioned above, episodes of the external factors in active attacks, in passive mode discussed. The person will

not have any effect on the source or destination system , But the text encrypted, and in some cases, text will be changed by the attacker. By using modern methods of encryption, can prevent such attacks, by using deterministic encryption methods, such as private-key encryption, public key encryption can stay away from complex functions which can be disabled the attacks

VII. Conclusion

E-Learning used modern technologies and new methods to improve its services, that the latest technology is cloud-based E-learning, which used this technology to provide better educational services. However the use of these technologies always appeared challenges and difficulties. These security challenges can be noted as the most important difficulties. One of the causes of the security challenges is using the cloud computing for data transferring in the internet that caused all Internet security threats in the cloud.

Thus the use of the internet and the lack of adequate security and a lack of consumer confidence due to the emerging cloud technologies is an obstacle to the development of this technology, particularly in the field of cloud-based E-learning. According to research and topics, suggested to service providers and governments to move and recovered data transfer mechanisms and protocols by using new techniques to be safe users' data which are the most important asset to the user in the cloud-based E-Learning. Because security holes in new techniques are optimal and minimal in data transfer protocols. Also, to overcome the security challenges in cloud-based E-learning, vendors and researchers have keep possible alternatives in cloud services for all manner of threats, to provide more cloud-based customers who desire to use cloud-based E-learning. Besides these things it should be consider security of infrastructure such as servers, because security servers can play major role in the cloud-based E-learning. Because the main concern of consumers in this model of technology is security of servers and data servers based on the secure servers which seems necessary. Threats that can compromise servers to cloud-based E-learning should be noted to authentication enhancement requests and availability. In order to overcome these security threats on servers such as Disaster Recovery, physical security and management standards security, can use security measures. In addition to provide secure servers, providing the security of E-learning users who are the beneficiaries of cloud-based E-learning is also crucial and vital. So security threats, such as browser security, authentication and authorization of the user of E-learning, security measures have done to overcome on threats such as security mechanisms SMS, digital signatures, security tokens, biometric mechanisms, etc.

References

[1] Y. Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science & Emerging Technologies, Vol. 2, No. 5, 2011, pp. 316-322.

[2] M. Al Morsy, J. Grundy and I. Müller, "An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 Nov 2010.

[3] H. Takabi, J. B. D. Joshi, G.Ahn., "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security Privacy Magazine, Vol. 8, IEEE Computer Society, 2010, pp.24-31.

[4] M. Monsef, N. Gidado, "Trust and privacy concern in the Cloud", 2011 European Cup, IT Security for the Next Generation, 2011, pp.1-15.

[5] M. Firdhous, O. Ghazali, and S. Hassan, Trust and Trust Management in Cloud Computing – A Survey, Inter Networks Research Group, University Utara Malaysia, Technical Report UUM/CAS/ InterNetWorks/TR2011-01, 2011.

[6] F. S. Gharehchopogh, S. Hashemi, "Security Challenges in Cloud computing with More Emphasis on Trust and Privacy", International Journal of Scientific & Technology Research, Vol. 1, ISSUE 6, 2012. pp. 49-54.

[7] J. Che, Y. Duan, T. Zhang, J. Fan, "Study on the security models and strategies of cloud computing", Procedia Engineering, Vol. 23, Elsevier, 2011, pp. 586-593.

[8] D. Jamil, H. Zaki, "Security Issues in Cloud Computing and Countermeasures", International Journal of Engineering Science and Technology, Vol. 3 No. 4, 2011, pp. 2672-2676.

[9] S. Qaisar, K. F. Khawaja, "Cloud Computing: Network/Security Threats and Countermeasures", Interdisciplinary journal of contemporary research in business, Vol.3, No. 9, 2012, pp. 1323-1329.

[10] Vic (J. R.) Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical Editor Bill Meine, Elsevier Publishing, 2011.

[11] G. Kumar, A. Chelikani, Analysis of Security Issues in Cloud Based E-Learning, Master's thesis, University of BORAS , Sweden, 2011.

[12] Kumar, A., Pakala, R., Ragade, R. & Wong, J., The virtual learning environment system. IEEE, vol. 2., 1998, pp. 711-716.

[13] V. Harmelen, M. Year. Personal learning environments. Sixth IEEE International Conference on Advanced Learning Technologies ICALT06 (2006), Volume: 16, Issue: 1, Publisher: Ieee, 2006, pp.815-816.

[14] P. Pocatilu, "Cloud Computing Benefits for E-learning Solutions", Oeconomics of Knowledge, Vol. 2, Issue 1, 2010.

[15] S. Hameetha Begum, T. Sheeba, S. N. Nisha Rani, "Security in Cloud based E-Learning", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 1, 2013, pp.1-6.

[16] Pocatilu, P., Alecu, F. & Vetrici, M., "Using cloud computing for E-learning systems", World Scientific and Engineering Academy and Society (WSEAS), 2009, pp. 54-59.

[17] Al-Jumeily, D., Williams, D., Hussain, A. & Griffiths, P., Can We Truly Learn from A Cloud Or Is It Just A Lot of Thunder? Developments in E-systems Engineering (DESE), 2010 pp. 131-139.

[18] RAO, N. M., Sasidhar, C. & Kumar, V. S, Cloud Computing Through Mobile-Learning, [Accessed Feb 2012] http://arxiv.org/ftp/arxiv/papers/1204/1204.1594.pdf

[19] G. Srinivas Reddy, Security Issues and Threats in Educational Clouds of E-Learning: A review on Security Measures, Int.J.Computer Technology & Applications, Vol 4 (2), 2013, pp.312-316

[20] Jamil, D. & Zaki, H., Cloud Computing Security, International Journal of Engineering Science and Technology (IJEST), Vol. 3, No. 4 pp: 3478- 3483, April 2011.

[21] Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L. L, On technical security issues in cloud computing, Cloud Computing, 2009. CLOUD '09. IEEE International Conference, Bangalore, 2009, pp.109 – 116.

[22] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J., Controlling data in the cloud: outsourcing computation without outsourcing control. , Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009); Chicago, 2009, pp. 85-90.

[23] Ahmed, S., Buragga, K. & Ramani, A. K. "Security issues concern for E-Learning by Saudi universities", Advanced Communication Technology (ICACT), 2011 13th International Conference, IEEE, Seoul-korea, 2011, pp. 1579-1582.