International Journal of Information Technology and Management

Vol. IX, Issue No. XIV, November-2015, ISSN 2249-4510

AN ANALYSIS UPON VARIOUS SECURITY PROBLEMS IN CLOUD BASED E-LEARNING ENVIRONMENT

International Journal of Information Technology and Management
Vol. IX, Issue No. XIV, November-2015, ISSN 2249-4510

An Analysis upon Various Security Problems in Cloud Based E-Learning Environment

Mohammed Khalid Kaleem[1]* Dr. Manaullah Abid Husain[2] Dr. Suneel Dubey[3]

[1] Research Scholar, Maharishi University of Information Technology, Lucknow, India

[2] Associate Professor, Department of Electrical Engineering, Jamia Millia Ismalia, New Delhi, India

[3] Associate Professor, Dept. of Computer Science & Information Technology, Maharishi University of Information Technology, Lucknow, India

Abstract – E-Learning with the techniques of Cloud system is the most upcoming technology in IT field and many e-learning products can be established with the aid of cloud computing technology. Cloud computing environment gives very comfort and flexible functions invented in e-learning product, security is a major issue to be analyzed in e-learning at cloud based technology. So security issues and measures are the compulsory and essential to maintain secrecy of the users' valuable data base stored in cloud servers.

E-learning is computer enhanced learning. It is blend of learning services and technology to provide high values. Educational services that provide e-learning system need hardware, software and substantial investment for the same. In order to reduce costs, these services can be provided based on cloud technology. Cloud computing is a technology of storing and accessing of data over the cloud (internet) instead of personal computer hard disk or local servers. This paper discusses how cloud computing environment has raised as a best platform in providing e-learning services. At the same time it also gives a description of cloud architecture for electronic based learning. This paper presents an environment derived from both virtual and personal learning environments based on cloud computing which contains tools and techniques to enhance the education process. At the end, this paper also discusses the various issues to be focused, challenges in cloud based e-learning and the benefits of e-learning based on cloud computing.

This study identifies different security issues in cloud service delivery model with an aim to suggest a solution in the form of security measures related to the cloud based e-learning. Different types of attacks in service delivery models of e-learning proposed by different researchers are dis-cussed. Threats, security requirements, and challenges involved are also taken into consideration. This study of e-Learning models advocates users to access their data in the cloud through a secured layer using the internet.

- - - - - - - - - - - - - - X - - - - - - - - - - - - - -

INTRODUCTION

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. At present, e-learning has become a widely accepted learning model and it provides innovative changes in learning system. However it needs a lot of investment without capital gains to return and staying power usually, education institutions cannot afford much in hardware and software resources investments. Cloud computing is the best solution and has been a hot topic due to its dynamic scalability and effective usage of the resources; it can be utilized effectively when the availability of resources is limited. However, besides the benefit it also involves security issues.

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

Therefore, 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. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure.

Each type of cloud computing model—public, private or hybrid—faces different levels of IT risk. In the private cloud delivery model, the cloud owner does not share resources with any other company. Private clouds are owned and operated by a single organization, delivering IT services within the constraints of their own network perimeter. In the public cloud computing model, IT activities and functions are provided as a service that can be billed on a pay-per-use or subscription basis via the Internet from external suppliers, using resources not owned by the consumer. The sharing of IT resources in a public, multitenant environment can help improve utilization rates and can reduce costs significantly, while maintaining access to high quality technology. In a public cloud, an organization rents IT resources instead of having to invest in their own physical IT infrastructure or maintain under-utilized equipment to service peak loads.

Instead, they can scale usage up or down, according to need, with costs directly proportional to need. Many organizations embrace both public and private cloud computing by integrating the two models into hybrid clouds. There are many advantages with replacement of traditional E-Learning method by cloud computing technology. Cloud based e-learning solutions play a vital role in reducing the cost of the traditional e - learning technology by its widespread cloud source. But still, there seems to be some problems that need to be concerned at the implementation of cloud based E-Learning solutions in all academic organizations. Many cloud computing companies come forward provide services to many technical solutions to make their products more cost effective. The E - learning is one of such technologies with an implementation of the cloud power to enhance the functionality for providing to e-learners. E-learning is one of the widespread technologies, which helps to share the knowledge among teachers and universities in academic sphere. At the time of cloud services, it is very essential to consider security issues. So in this paper, the key security issues in the utility of cloud computing in e-learning processes have been studied. Security is a just most important all stages of cloud service. Security issue needs to be more focused when system involves the gadgets or technologies with internet. The present work is approached with modern techniques for enabling the cloud service in E-learning process at more advances facilities for the customers as compared to normal existing system. Cloud computing is one of the emerging technology which gives more benefits in the business domain and other applications. Still the cloud environment is of no perfect security in its functional platform. The present study will focus on the security in E-learning with cloud implementation.

Individual learning environment (ILE) is simply mechanism of the E-Learning systems through computer applications with web sources. Individual learning technique is a great innovative application with a modern mechanism with cloud network. The task of INDIVIDUAL LEARNING is to provide virtual class room environment huge number of students in worldwide. The terms similar to Individual learning environment are learning management system (LMS), Content management system (CMS), Learning content Managed learning environment (MLE). Individual learning environment basically depends on the on the internet and it provides the learning tools to e-learners for uploading files, chatting, and web conferencing. This learning process gives the advanced and provisions at precise level

- A general display for update information of the course work.
- Courses are available at any time and any convenient place to students.
- Certain needs and restrictions are framed in this kind of e-learning systems.
- The system of cloud in education domain gives a support the people in areas at geographically wider separation.
- Education with cost effective and flexible is possible.

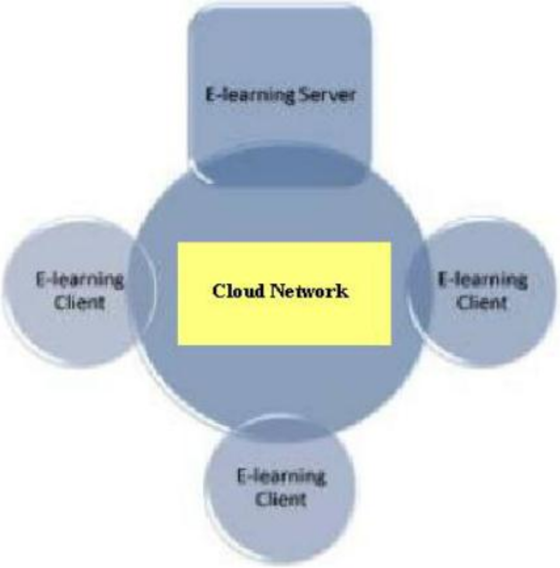

Figure 1. Basic outline of cloud for e-learning.

The figure 1 reveals basic connectivity of the blocks required for the process of e-learning with the cloud technique.

E-Learning is one of the most significant technologies which help institutions to create a good learning environment. With the help of internet, it is possible to adopt e-learning system at low cost with minimum expenditure. Problems related to the security issues render greater constraints for cloud vendors and users. Various combinations of signal transmission techniques, advanced web technologies and other hardware developments which establishes secure e-learning1,2. The introduction of cloud computing technology in e-learning shows many advantages over the existing e-learning methodologies in infrastructure and cost wise3. This cloud e-learning technology is considered to be a proper replacement technology over traditional e-learning. The security is the major issue in the cloud computing or on demand cloud computing model. In a survey conducted by IDC on 224 IT executives, the security is marked as 74.6% which is as shown in Figure 1.

In this paper, we provide a brief but well-rounded survey on cloud security trends. We recognize that there are three cloud service delivery models 1. SaaS, e.g. Google apps, salesforce.com, zoho.com 2. PaaS, e.g. Google App engine, force.com, Microsoft Azure 3. IaaS, e.g. Amazon, IBM, Rackspace Cloud in which cloud security is involved. This paper tried to map security concerns and obligations of each of these groups. We observe that data, platform, user access and physical security issues; although emphasized in cloud computing; are generally applicable in other enterprise computing scenario as well. For example, hypervisor related threats such as cross channel attacks are present in any virtualized environment and it is not specific to cloud computing4,5. Two of the great virtues of cloud computing are service abstraction and location transparency. However, from security point of view these two points in conjunction with third-party control of data can create challenging security implications. The paper outlines how secure cloud environment, impact of security threats, and comparative study on security threats.

Cloud computing employs three service delivery models as listed below through which different types of services are delivered to the end user. Each service model has different levels of security requirement in the cloud environment. They are,

A. Software as a Service (SaaS)

B. Platform as a Service (PaaS)

C. Infrastructure as a Service (IaaS)

These models provide Software, application platform and infrastructure resources as a service to the users. The Figure 2 shows the different types of attacks involved in these service delivery models.

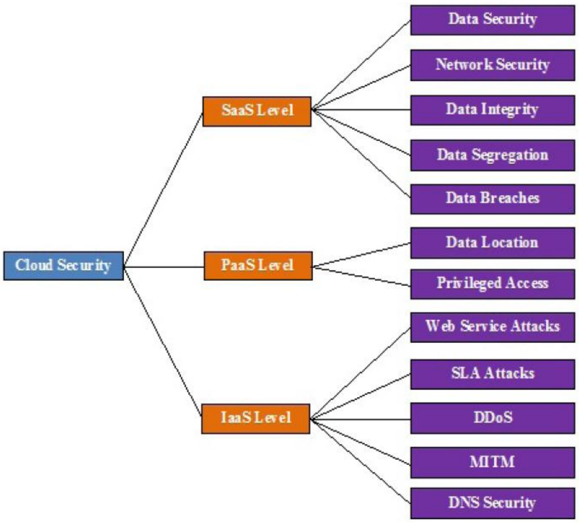

Figure 2. Types of Security attacks in Cloud based E-Learning.

In SaaS, the client has to depend on the provider for proper security measures. The provider must do the work to keep multiple users' from seeing each other's data. So it becomes difficult for the user to ensure that right security measures are in place and it is also complicated to get assurance that the application will be available when needed6 to avoid the risks of maintaining high availability problems by having multiple copies of the data at several locations throughout the country.

In Platform as a service, cloud computing provides computing platform and system software as a service. Cloud users create an application by controlling software deployment and configuration settings from the providers. When we look at security point of view, host based, and network based intrusions are challenging factors of PaaS Providers13. The major PaaS level security threats are in Data Location and Privileged access.

Infrastructure as a service model allows for variety of resources such as servers, storage, networks, and other computing resources are as virtualized systems, which are getting access through internet. Users can run any software with security on the allocated resources, so IaaS provides full control and management on the resources. Hence, cloud providers are only the responsible for configuring security policies. Some of the security issues associated to IaaS are: Web service attack, SLA Attack, DDoS Attack, MITM Attack and DNS Attack.

E-LEARNING BASED ON CLOUD COMPUTING

The educational cloud provides a magical solution the educational institutes and organization who want to switch to e-learning system. They have the choice to select either to build a private cloud or go to a cloud service provide to share the resources after defining parameters. Before transforming e-learning system to cloud, first and foremost you need to identify which services you need and create a service catalogue for the same in order to determine the parameters you need from the service provider. Cloud based elearning includes hardware and software resources to develop the traditional e-learning infrastructure. Cloud based E-learning architecture mainly consists of five layers which are described below:

Hardware Layer: This layer handles the important hardware resources like CPU, physical memory. Physical servers, network and storage are grouped with the help of virtualization. Dynamic expansion of physical host is possible and memory is scalable at any time to supplement additional memory in order to offer uninterrupted power to cloud middleware services for the e-learning system based on cloud computing.

Software Resource Layer: Middleware and operating systems are used to create this layer. By combining various software solutions with the help of middleware technology, software developers are provided with grouped interface**.** Software developers can develop applications for e-learning system and embed them in the cloud. Cloud users can access those applications through cloud.

Resource Management Layer: It play a major role to get loose coupling of hardware and software resources. By using virtualization and scheduling concept of cloud computing, this layer provides uninterrupted on demand software distribution for different hardware resources.

Service Layer: This layer helps the cloud clients to use different forms of cloud resources. Service layer is classified as three layers: IaaS, PaaS, and SaaS

Business Application Layer: This layer is different from the other four layers of cloud based e-learning architecture. It consists of education platform, content creation, content delivery, teaching and evaluation and education management.

E-learning system based on cloud computing uses the services in three ways:

1. Infrastructure – use an e-learning solution on the provider's infrastructure.

2. Platform – use and develop an e-learning solution based on provider's development interface.

3. Services – use the e-learning solution given by the provider.

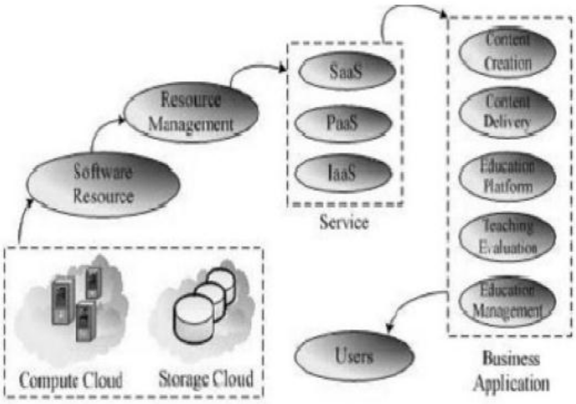

Fig. 3: Cloud based e-learning architecture.

CHALLENGES IN CLOUD BASED E-LEARNING:

- Security and Privacy: The major challenge of cloud computing is the way it addresses the security and privacy issues. Cloud infrastructure would get affected even if one site is attacked. These risks/threats can be diminished by using encrypted file systems, security applications, and security hardware to track unusual attack across the servers.

- Currently cloud service providers are adopting proprietary API's to implement their applications. Consequently, services transition from one service provider to another has become extremely complicated and consumes time.

- Enterprises may not be aware of where the cloud servers are located and from technology point of view, location of data is not relevant. But this has become a critical issue for data governance requirements.

- Businesses/Enterprises can save money on hardware but they need to spend more for the bandwidth in order to deliver intensive and complex data over the networks. Therefore, clients are waiting for the reduction in cost before switching to cloud.

- The service level agreements of the cloud service provider are not adequate to guarantee the availability and scalability. Clients will be reluctant to switch to cloud without a strong quality guarantee.

SECURITY IN CLOUD BASED E-LEARNING

Security is one of the primary concern in the greater context of cloud computing as it relates to cloud based e-learning. From 2005-2011, security has been in the top four IT issues as published by Educause, a “nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology”. When shifting e-learning in the cloud, main security concerns are about confidentiality, integrity and availability. Security remains as an integral component of the top ten IT issues in 2012**.**

A. *Seven Threats to security in cloud computing*

There are several significant threats that should be considered before adopting the paradigm of cloud computing in e-learning. These threats are described as follows:

1) *Abuse and Nefarious use of cloud:* Cloud services providers often targeted for their weak registration system and limited fraud detection capabilities. This paves way to the spammers, malicious code authors and other cybercriminals can misuse the various types of services including unlimited bandwidth and storage facilities offered by the cloud providers. Misuse includes creating spam, decoding and cracking of passwords, executing malicious codes to access rich information such as question papers, learning materials, assessments etc.

2) *Insecure Software Access:* Various software interfaces and APIs are used by the cloud users in e-learning to access and manage the cloud services. These APIs play an integral part during provisioning, management, orchestration and monitoring of the processes running in a cloud environment. Hence these APIs needs to be secured and should include features of authentication, access control, encryption and activity monitoring. Many security issues will be raised if cloud service providers believe on weak set of APIs.

3) *Malicious Insider:* Malicious employees who are working in the provider’s or user site can be able to perform insider attacks. This insider can steal the confidential data of cloud users in e-learning. Malicious insider can easily get the cloud users in e-learning confidential data such as password, cryptographic keys and files. It will affect the standards and trust of cloud users in e-learning. As a result, it can cause damage on both financial grounds as well as organisation reputation

4) *Data Separation:* Virtual Machine (VMs) are virtualized based on the physical hardware of cloud providers and stores the e-learning user’s applications supplied by the cloud providers due to the cloud virtualization. These VMs are isolated from each other by cloud providers in order to maintain the security of users. These VMs are managed by hypervisor who are the main source of managing the virtualized cloud platform so as to provide virtual memory as well as CPU scheduling policies to VMs. Hypervisors are mainly targeted by the hackers since they are residing between VMs and hardware. Strong isolation is needed to ensure that VMs are not able to access the activities of other VMs under the same cloud computing providers. Even though several vendors offers strong security mechanism to protect the cloud supervisors, however sometimes security of VMs is compromised

5) *Data Loss or Leakage:* Operational failures, unreliable data storage and inconsistent use of encryption keys will lead to a data loss. Operational failure includes deletion, incomplete deletion or alteration without any backup of the source e-learning content. It may be either intentionally or unintentionally. Unreliable data storage means storing a data on unreliable media which cannot be recoverable if the data is lost. Inconsistent use of encryption keys will lead to unauthorized access and data loss such as destruction of sensitive and confidential information. It will definitely affect the reputation of the company.

6) *Hijacking:* Controlling the users account through the unauthorized access by the hackers is referred as account or service hijacking. It includes phishing, fraud and exploitation of software vulnerabilities. It is not enough to secure the sensitive and confidential information through the common way of authentication and authorization process e-learning.

7) *Unknown Risk:* It is essential for the every e-learning user to know the software versions, security practices, software code updates and intrusion attempts. Cloud service providers usually advertised these futures and functionality with the necessary details such as internal security procedure, configuration hardening, patching, auditing and logging. E-learning users must be aware and clarified how their data and related files are stored. On the other hand, e-learning user may unaware of the unknown risk profile which may include serious threat.

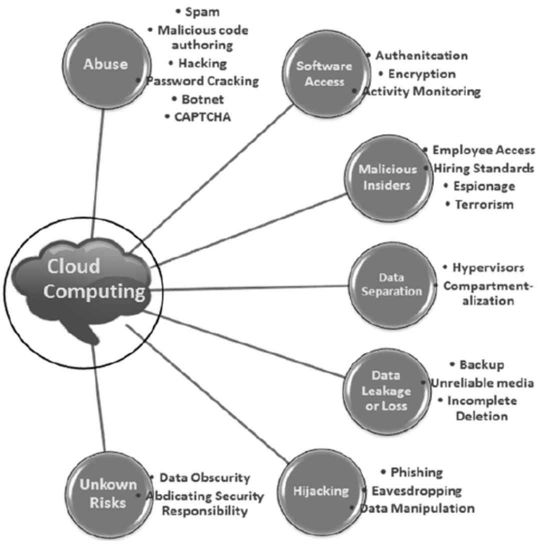

Fig. 4 Seven threats to security in cloud.

ISSUES IN SECURITY CHALLENGES AT CLOUD ENVIRONMENT

All printed Security aspects are to be considered in ensuring confidentiality of the proposed system in the cloud users to handle it for its dependency on the web sources in the operation, there are plenty of threats to attack in cloud based e-learning technology through the internet. Even though cloud provides numerous advantages to e-learners, the cloud security remains still doubtful for its security issues and challenges in a digital world. Many multinational organizations now come forward in cloud services. All these companies are of good name in giving reliable services to users, but still peoples don’t have the confidence about cloud security system from those companies. So those companies are in necessity of framing the different possible security measures in cloud services. In the same time, security in e-learning materials also becomes an essential step to be taken in the system of e-learning process. The discussion in the paper is made on issues and security mechanisms In many countries, large part of the financial budget is allotted for developments in education sector and a considerable focus is now on the e-learning systems. The internet facilitates e-learning opportunity for majority of the people across the country at low cost and minimum expenditure. Along with the development of the advanced facilities in the spreading the knowledge for the people across the nation through internet, problems related to the security also raises that needs to be considered very seriously for mitigation through the implementation of the possible security techniques and processes. With several combinations, such as signal transmission techniques and advanced web technologies and other hardware developments, it is found that e-learning is well established. The people at different locations are provided the facility of learning simultaneously in a more comfort and flexible ways.

As there are many facilities available for different domains in the technological fields, cloud process needs to consider more and more tasks for the framing of security mechanisms. There are many challenging points in maintaining the security methods as given under:

Primary security considerations - It is required to involve in the system the awareness or control of running criteria over the utility of the resources as they are being shared by the customers of third party. Most of the services are not of the similarities in characterizations with that from 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. During the cloud services it is must to maintain a 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 hence a combined method of these functions needs to be associated with certain standards.

Data Lock-in - Data fixed in certain format by a particular cloud vendor cannot be transferred to the other, and it causes data lock-in. A continuous service needs to be provided with this lock-in system. And more technological updates are also necessary for the fixation of the data format so as to be convenient transaction of information in other cloud vendors.

Deletion of the in secured and incomplete data - The permanent removal of information from the machine after an operating instruction is over makes the customer feel secure. This is one of the most challenging tasks to be monitored in cloud security system.

Increased demands security policy - With the facility that accessing the software without installation in machine and supported by the cloud server, it is very essential that a system of authenticity for accessing the software is to be established carefully to its authorized users. If the system fails to monitor reliability in maintaining the authenticated process, it may cause insecure problems in the usage of applications.

Browser security - Each assignment of the application process in cloud system needs to take the centralized servers. Since the browsing system is the only tool for customer to use cloud service, it is more important that modem web browsers needs to be framed and designed with certain standards of security mechanisms which can be possible by XML signature and XML encryption.

Over the sensitive data, cloud vendors are to be responsible for the leakage of data to the unauthorized users. A continuous monitoring on updation of security mechanism for the sensitive information must be made.

CONCLUSION

The interesting conclusions are drawn from the study of the survey and empirical analysis. But the main key point in cloud based e-learning is to maintain security system as shown in the empirical studies. Some key security issues in cloud based e-learning technology are emphasized specially. Security management standards are helps to ensure the safety in mindset of customers**.** The present study suggests security certain management standards for safety processing of the cloud based learning. It will raise the CBE users without any fear over its security. And also various security measures are suggested in the empirical study are used to overcome the security threats in CBE technology.

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.

E-learning systems are facing challenges with respect to services, media content, and instruction resources with the huge demand and growth of users. Cloud Computing has emerged as an appropriate platform to migrate from e-learning system. There are certain challenges and issues like security, data lock-in, and bandwidth are faced by cloud based e-learning. But still the customers/clients/users are getting attracted towards switching to cloud computing. The benefits and features of cloud based e-learning are overtaking the drawbacks.

REFERENCES

A.B. SmithPocatilu, P., Alecu, F., Vetrici, M (2010). Measuring the efficiency of cloud computing for e- learning systems. W. Trans. on Comp. 9, pp. 42–51.

Begum SH, Sheeba T, Rani SNN (2013). Security in cloud based 4. E learning. Int J Adv Res Comput Sci Software Eng. 3(1).

D.Kasi Viswanath, S.Kusuma and Saroj Kumar Gupta (2012). “Cloud Computing Issues and Benefits Modern Education”, *Global Journal of Computer Science and Technology Cloud & Distributed*., Vol. 12 Issue 10 Version 1.0 pp.15-19, July 2012.

D.Kasi Viswanath, S.Kusuma and Saroj Kumar Gupta (2012). “Cloud Computing Issues and Benefits Modern Education”, *Global Journal of Computer Science and Technology Cloud & Distributed*., Vol. 12 Issue 10 Version 1.0 pp.15-19, July 2012.

G. Reddy, "Security Issues and Threats in Educational Clouds of E-Learning: A review on Security Measures, " *International Journal of Computer Technology and Applications.*

Gharehchopogh FS, Hashemi S. (2012). Security challenges in 8. Cloud computing with more emphasis on trust and privacy. International Journal of Scientific and Technology Research; 1(6): pp. 49–54.

K. m. Seyyed Yasser Hashemi, "E-learning Based on Cloud Computing: Issues and Benefits, " *MAGNT Research Report,* vol. 2, pp. pp. 104-109.

Md. Anwar Hossain Masud, Xiaodi Huang (2012). “An E-learning System Architecture based on Cloud Computing”, *World Academy of Science, Engineering and Technology 62.*

Mervat Adib Bamiah & Sarfraz Nawaz Brohi, (2011) .“Seven Deadly Threats and Vulnerabilities in Cloud Computing”, International Journal Of Advanced Engineering Sciences And Technologies, Vol No. 9, Issue No. 1, pp. 87 – 90

Mervat Adib Bamiah & Sarfraz Nawaz Brohi, “Seven Deadly Threats and Vulnerabilities in Cloud Computing”, *International Journal Of Advanced Engineering Sciences And Technologies*, Vol No. 9, Issue No. 1, pp. 87 – 90,

Piplode R, Singh UK (2012.) An overview and study of security 14. issues and challenges in cloud computing. Int J Adv Res Computer Science Software Eng. Sep; 2(9).

S. Y. H. Sajjad Hashemi (2013) "Cloud Computing for E-Learning with More Emphasis on Security Issues, "*International Journal of Computer, Information, Systems and Control Engineering,* vol. 7, no. 9.

S. Y. H. Sajjad Hashemi (2013). "Cloud Computing for E-Learning with More Emphasis on Security Issues, "*International Journal of Computer, Information, Systems and Control Engineering,* vol. 7, no. 9.

Takabi H, Joshi JBD, Ahn G. (2010). Security and privacy chal5. lenges in cloud computing environments. IEEE Security Privacy Magazine. IEEE Computer Society. 2010; 8: pp. 24–31.