Volume 3, Issue 1, January 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security in Cloud based E-Learning

S.Hameetha Begum[*]
Computing&Muscat College
Oman

T.Sheeba
Computing &Muscat College
Oman

S.N.Nisha Rani
ECE &Fatima Michael Engg. College
Tamilnadu, India

Abstract*—E-learning is a form of learning created by combining digitally delivered content with learning support and services.E-learning systems usually require many hardware and software resources. Educational organizations cannot afford huge investments to obtain these resources. Cloud computing is the best solution as it delivers the computing resources (hardware and software) as a service over the internet. It provides resources and capabilities of information technology via services offered by CSP (cloud service provider).This paper mainly focuses on the influence of cloud computing concepts in an e-learning system. In addition to that, this paper also discusses the security threats in cloud based e-learning systems and the guidance provided by the eminent companieslike Intel, Microsoft in solving these threats.

***Keywords*— E-learning, Cloud Computing, CSP, Security Threats,Intel,Microsoft**

I. 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[1]. 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 returnand 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 [2][3].

This paper is organized as follows. Section II describes cloud computing, its benefits, service model, service deployment model and its challenges. Section III demonstrates cloud based e-learning, its architecture and what benefit cloud computing can provide to an e-learning system.Section IV explains the security threats in cloud based e-learning.Section V describes guidance of security concern in cloud computing and Section VI is the conclusion.

II. CLOUD COMPUTING

Organisations prefer to minimize their investment on hardware resources and IT maintenance as it involves higher operational expenses.Business activities such as operations, marketing, production and administration can run efficiently with the help of these IT services. Organisation cloud computing has become one of the hottest buzz word to provide the solution for this problem in today's IT world. Organisation can get theseservices via internet from third party organisation when needed.In turn, organisation has to pay the service provider for using their services and there is no need to spend any money to build and maintain their IT infrastructure as this could be achieved with the help of cloud computing.

Some of the definitions of cloud computing are as follows:

A. Definitions and Benefits

Cloud Computing [4] is a computation paradigm in which the resources of an IT system are offered as services available to the users through net connections, frequently the internet. Cloud computing[5]is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet).It entrusts remote services with a user's data, software and computation**.** Cloud computing [2] is a computing model based on networks, especially on internet, whose task is to ensure that users can simply use the computing resources on demand and pay money according to their usage by a metering pattern similar to water and electricity consumption. Therefore, it brings a new business model, where the services it provides are becoming computing resources. It is highly scalable and creates virtualized resources that can be made available to users. Users do notrequire any special knowledge about the concept of cloud computing to connect their computers to the server whereapplications have been installed and use them. Users can communicate through Internet with remote servers. Theseservers can exchange their computing slots themselves.

Cloud computing allows to move the processing effort from the local devices to the data center facilities. Some of the clear benefits that the cloud computing fetches for any type of organisations is given below [6][7][8]:

1) *Cost reductions:*It helps to reduce capital cost, operational expenses like implementation and maintenance costto a great extent.
2) *Automation:*Automation is the one of the greatest attraction of this technology. Businesses do not need to set up a team to handle system updates and back-ups,which help to free up internal resources.Moreover, other higher priority work can be released through internal sources.
3) *Mobility:*It helpsto mobilize the businessesdramatically to grow and succeed. Employees can access work-related information from anywhere and it helps in increased mobility for a global workforce.
4) *Flexibility:*It allows dynamic scalability as demands fluctuate.
5) *Time saving:* As cloud computing becomes functional faster than other systems, businesses save precious time. Recoveries are also fast with cloud computing and product will get faster into the market with the help of cloud computing system.
6) *Accessibility:*It helps to make data and services publicly available without making vulnerable sensitive information.
7) *No Complications:*Businesses with different technologies will make the system more complicated. In comparison to the other systems, installation of cloud computing is easier. Additional hardware or software is not required by the organisation. Putting into effect is not too complicated as it is done remotely. Since, the data's are stored in the cloud server, there isalmost no data lost even if the client computer crashes.
8) *Reducing the paper work:* "Greening" of the data center. It encouragesreducing the paper worksin the data center.
9) *Availability:*Increased availability of high-performance applications to small/medium-sized businesses.

B. Cloud Computing Service Models

Cloud computing service models comprises of three layers[4]:infrastructure as a service (IaaS), platform as a service (PaaS)and software as a service (SaaS).

*1) Infrastructure as a Service (IaaS):*IaaS provides hardware as a service through virtual machines or other resources such as servers, virtual local area networks, storage or computation, as well as basic characteristics such as operating systems and virtualization of hardware resources.i.e., cloud service providers offers all the required hardware resources and the client uses their own scale services up and down according to their requirements to run their business effectively.

2) Platform as a Service (PaaS): At the PaaS level, the provider supplies more than just infrastructure, i.e. an integrated set of software with all the stuff that a developer needs to build applications, both for the developing and for the execution stages.

3) Software as a Service (SaaS): In the last level,SaaS is foundto offer software as a service. This was one of the first implementations of cloud services. It has its origins in the host operations carried out by the application service providers, from which some companies offered to others the applications known as customer relationship managements.If the organisation only need to use a specific kind of software to get specific desired output then it is much cheaper to use the service from a cloud provider rather than purchasing the software.

C. Cloud Computing Deployment Models[9][10]

*1) Public cloud:*In public cloud, the cloud infrastructure is owned by an organization selling cloud services. The infrastructureand other cloud services are made available to thegeneral public over the internet. The cloud is ownedand managed by a CSPwho offers services toconsumers on a pay-per-use basis. Users are by default treated as untrustworthy;therefore, security and privacy are big concerns about this type of cloud. Many popular cloudservices of public cloud include Amazon EC2, Google App Engine and Salesforce.com.

*2) Private cloud:*In private cloud, the cloud infrastructure is owned or leased by a single organization. The computingresources are operated exclusively by oneorganization. It may be managed by theorganization itself or a cloud service provider. Private clouds areconsidered to be more secure than public cloudssince their users are trusted individuals inside theorganization. The other two deployment models,community clouds and hybrid clouds, fall betweenpublic and private clouds.

3) Community cloud:In community cloud, the cloud infrastructure is shared by several organizations that has shared concerns.It issimilar to private clouds but the cloud infrastructure and computing resources are shared by several organizations that have the same mission, policy and security requirements. An example of acommunity cloud is the educational cloud used by universities and institutes around the world to provide education and research services.

4) Hybrid cloud:In hybrid cloud, the cloud infrastructure is a composition of two or more clouds that remain unique entities. The cloud infrastructure consists of a combination of two or more public, private or community cloud components. The cloud components are bound together by standardized technology and managedas a single unit, yet each cloud remains a unique entity. It allow organizations tooptimize their resources, so the critical core activities can be run under the control of the privatecomponent of the hybrid cloud while other auxiliary tasks may be outsourced to the public component.Fig. 1 below shows different cloud computing deployment models:

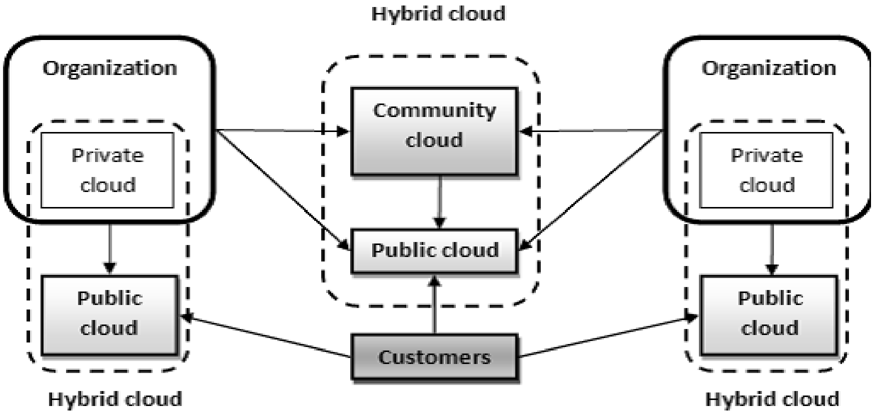

Fig. 1Different Cloud Computing Deployment Models[10]

D. Technological Challenges in Cloud Computing[4]

Cloud computing has shown to be a very effective paradigm according to its features such as ondemand self-services since the customers are able to use their services according to their requirement and it is mainly based on pay-per-use business model. However there are also some drawbacks are as follows which should be taken into consideration

1) Security, privacy and confidence: Since the data iscirculated over different servers, there is a necessity of an efficient and robust encoding method to manage the hardware for computation, when ‘uncontrollable’situation is faced by the client.Several audits and certifications of the security must be carried out to gain the confidence of the user.

2) Availability, fault tolerance and recovery: Redundant system is used to avoid the net traffic overflow and to guarantee a round a clock permanent service (24X7).

*3) Scalability:*An intelligent resource management is provided according to the user changing demands. Effectivemonitorization is done by identification of a priori the usage patternsandscheduling optimisation is done by predicting the load.

4) Energy efficiency: It is necessary to monitor the energy consumption of the processor.Using microprocessors with lower energy consumption assist in reduction of the electric charge and adaptable to their use.

III. CLOUD BASED E-LEARNING

E-learning is widely used indifferent educational levels such as continuous education, corporate trainings, academic courses, assessments etc. Many educational institutions do not have proper resources and infra structure needed to run the e-learning systems. Hence most of the institutions are using Blackboard and Moodle E-learning software to fulfil their needs. Nowadaysthissoftware’sare coming with versions of cloud oriented base applications.

A. E-learning Systems and its benefits[1][3]

E-learning systems are typically developed as distributed applications, but it is not limited to this application alone. The basic architecture of an e-learning systemincludes a client application, an application server and a database server (see Fig. 2). In addition to that necessary hardware components like client computer, communication infrastructure and servers are needed to support it.

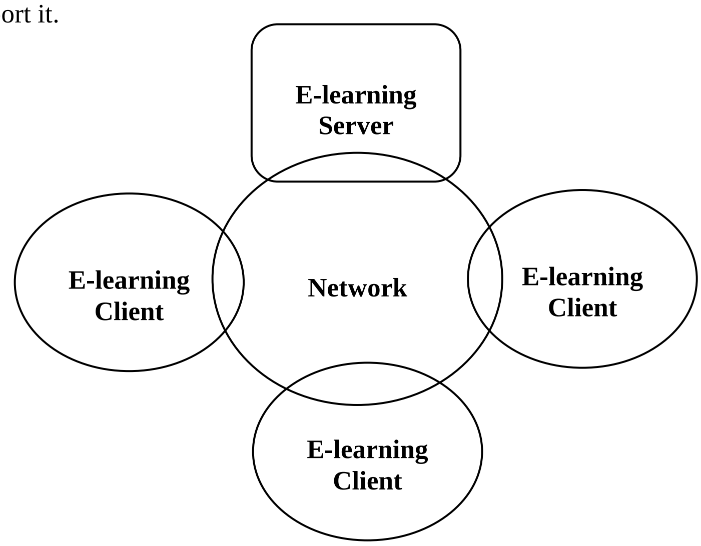

Fig. 2 Basic architecture of E-Learning systems[1]

E-learning has definite benefits over the traditional training method. There are various e-learning solutions available from open source to commercial.

1) Lower Cost: E-learning can be more cost effective to deliver than class room based training. It reduces the cost of training in organizations in terms of expertise trainer, course materials, travel and accommodation expenses.

*2) Time Saving:*It helps to save the time. Learners can learn what they need to learn and they can learn at their own pace irrespective of their capability i.e. slowest or fastest member of a group. At the same time it helps to reduce the time spent on travel.

3) Faster Delivery: It has faster delivery cycle times than traditional class room training as it is not limited to the specific number of classrooms and trainers. In traditional method, there are practical constraints of using available classrooms and trainers.

*4) Effective Learning:*It is helpful for the two important entities involved in an e-learningsystem: the students and the trainers.The students can take online course, exams,send feedback,homework and projects. At the same time trainers can deal with the content management, prepare tests, assess tests, homework, project etc.taken by students and communicate with the students through forum.

5) Lower environment impact: E-learning can also save trees by saving paper. Many e-learning courses are entirely self-contained, presenting all learning content online, or providing alternatives to paper-based forms of communication through toolssuch as email, PDF manuals, synchronous classrooms, and other web-based tools.

B. Architecture of Cloud based E-learning[1]

Cloud based e-learning is the sub division of cloud computing while it is helpful in education field for e-learning systems. It has a greater opportunity in the e-learning technology and its infrastructure prospects. Cloud based e-learning includes the hardware and software resources to develop the traditional e-learning infrastructure. The students can use the education materials of e-learning systems as it is virtualized in cloud server and others can also utilize this service on the rental basis from the cloud vendors. Cloud based e-learning architecture is depicted in the following figure:

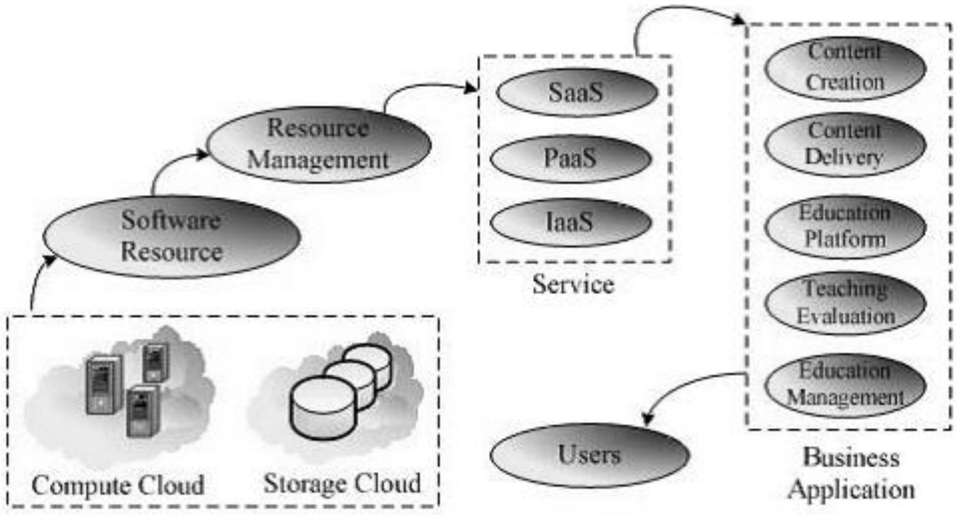

Fig. 3 Cloud based E-learning architecture[1]

Cloud based e-learning architecture[1] is mainly classified into five layers called hardware resource layer, software resource layer, resource management layer, server layer and business application layer.

*1) Hardware Resource Layer:*This is bottom most layerin the cloud service middleware and important for the total infra structure. It handles the essential computing hardware resources like physical memory and CPU. Physical servers, network and storage are grouped with the help of virtualization and it is called as anupper software platform. Physical host pool is expanded dynamically and memory is scalable at any time to add additional memory in order to offer the uninterrupted power to cloud middleware services for the cloud based e-learning systems.

2) Software Resource Layer: Operating systems and middleware is used to create this layer. Grouped interface is offered to the software developers by combining various software solutions with the help of middleware technology. Hence, software developers can develop many applications for e-learning system and able to embed those in the cloud which helps the cloud users to compute those applications through cloud.

*3) Resource Management Layer:*It plays a vital role to get loose coupling of hardware and software resources. It brings the uninterrupted on-demand software distribution for different hardware resources by means of virtualization and scheduling concept of cloud computing.

4) Service Layer: Service layer is categorized into three levels namely IAAS,PAAS,SAAS. It helps the cloud clients to use the various forms of cloud resources like software, hardware and infrastructure resources for their products.

*5) Business Application Layer:*This layer differs from all other layers in the cloud based e-learning architecture as it acts as an important business logic of e-learning and frames the expansion of group of components for e-learning. It mainly consists of content creation, content delivery, education platform, teaching evaluation and education management.

C. Benefit of cloud computing in E-learning systems[3]

E-learning Systems can use the benefit from the cloud computing using:**Infrastructure:** Use an e-learning solution on the provider's infrastructure, **Platform:** Use and develop an e-learning solution based on the provider's development interface and **Services:** Use the e-learning solution given by the provider.

Data security is a very big concern in the cloud computing since both the software and the data are located on remote servers that can crash or vanish without any additional warnings. Even if it seems not very reasonable, the cloud computing provides some major security benefits for individuals and organisations that are using or developing e-learning solutions as follows[3]:

*1) Improved Improbability:*It is almost impossible to determine where the machine is located which stores some important data such as test, exam questions, results etc.,for any person intended to steal these data. At the same time it is unattainable to find out which physical component he/she needs to steal in order to get a digital asset.

*2) Virtualization:*It makes possible for the rapid replacement of a compromised cloud located server without major costs or damages. Cloud down time is expected to be reduced substantially because it is very easy to create a clone for a virtual machine.

*3) 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 connectedveryfast.

*4) 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.

IV. 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 “non profit 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[11]**.**

A. Seven Threats to security in cloud computing[11][12]

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 codesto 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-learningconfidential 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 unauthorised 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.

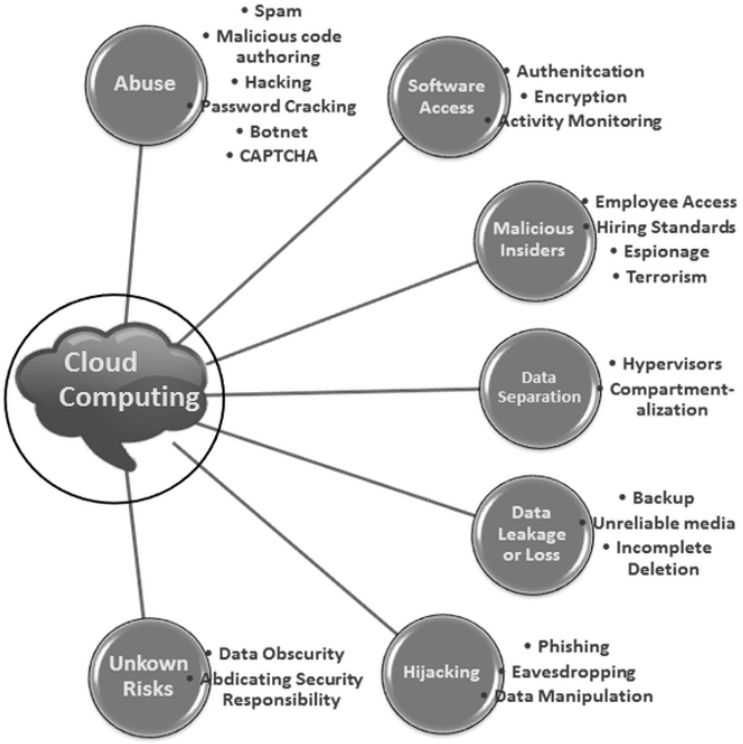

Fig. 4 Seven threats to security in cloud[11]

V. GUIDANCE FOR SECURITY CONCERN IN CLOUD BASED E-LEARNING

There are various steps given by the cloud service providers to ensure the security concern in the cloud computing which could be applied to cloud based e-learning. Few guidelineshave been given by the organizations such as Cloud Standards Customer Council, Intel,Microsoft etcto build the security in the cloud are as follows:

A. Cloud Standard Customer Council :Ten Steps of Security for Cloud Computing[13][14]

Cloud Standard Customer Council has published a white paper on “Security for cloud computing: 10 steps to ensure success” which include a list of steps, along with guidance and strategies, designed to help public cloud consumers evaluate and compare security provided in key areas from different cloud providers. This10 stepshas to be followed by the institutions to ensure the security for cloud computing before going for cloud services in their e-learning systems.

*1) Step 1: Ensure effective governance, risk and compliance processes:*Security controls available in cloud computing are very much similar to traditional IT environments. But educational institution should understand their own level of risk tolerance and focus on mitigating the risks that institutions cannot afford to neglect.

2) Step 2: Audit operational and business processes: Audits should be carried out by the educational institution appropriately by assigning skilled staff and set of controls should be established to meet the institutions security requirements.

*3) Step 3: Manage people, roles and identities:***Educational** institutions needs to control users' roles and privileges as it manage thousands of users such as students and staff who access cloud applications and services, each with different roles and rights.

*4) Step 4: Ensure proper protection of data and information:*Educational institution should ensure the proper protection of data and information. Additional focus on data security is needed because of the distributed nature of the cloud computing infrastructure and the shared responsibilities that cloud computing involves.

*5) Step 5: Enforce privacy policies:*Educational institutions are responsible for defining policies to address any privacy concerns and in increasing awareness of data protection within the institutions. In addition to that they should ensure the adherence of cloud providers to the defined privacy policies.

*6) Step 6: Assess the security provision for cloud applications:*Educational institutions must apply the same diligence to application security for both physical security and infrastructure security. Applications should not be compromised at any cost to avoid any additional risk.

*7) Step 7: Ensure cloud networks and connections are secure:*Educational institution should check for certain external network perimeter safety measures from cloud providers to ensure the secured connections and network.

8)Step 8: Evaluate security controls on physical infrastructure and facilities: Educational *institutions* should concern about the physical infrastructure and facilities provided by the cloud providers and it are an important consideration for security of any IT system especially in a cloud based e-learning. *9) Step 9 : Manage security terms in the cloud Service Legal Agreement(SLA):*As cloud services involves more than one organisation, responsibilities of user and the service provider must me made clear in SLA for better understanding. Educational institution should double check the terms in the SLA.

10) Step 10: Understand the security requirements of the exit process: Exit process must allow the educational institution to retrieve their data in a suitable secured form. It includes clarity on backup retention and deletion.

B. Intel's IT Center : Seven Steps for building security in the cloud[15][16]

Intel's IT Center(2012) has published a helpful guide for IT managers in ensuring best practices to follow in the cloud in order to help in building the security in the cloud.

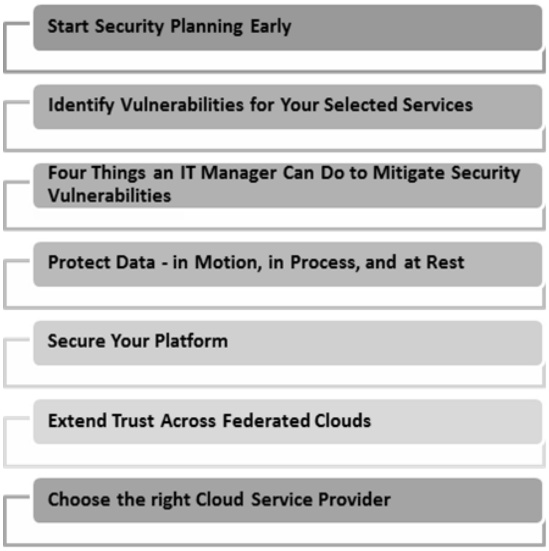
Start Security Planning Early
Identify Vulnerabilities for Your Selected Services
Four Things an IT Manager Can Do to Mitigate Security Vulnerabilities
Protect Data - in Motion, in Process, and at Rest
Secure Your Platform
Extend Trust Across Federated Clouds
Choose the right Cloud Service Provider

Fig. 5 Seven Steps of security for cloud computing[11]

1) Step 1: Start security planning early: The best way to approach cloud security is to integrate it with overall cloud planning early in the process. By this way, educational institution can use a threat based approach to planning for deployments of their specific workloads, security requirements and specific cloud delivery model and architecture.

*2) Step 2:Identify vulnerabilities for selected services:*It is the responsibility of the educational institution to identify the vulnerabilities for the selected services in the cloud computing. It is also important to understand while a fill-the-gap approach may seem to work on a particular vulnerability, but it may expose the unknown vulnerabilities in other areas.Best approach is to review the specific service architecture and then layer technologies to develop a strong security net that protects data, applications and platform and network at all levels irrespective of chosen cloud model.

*3) Step 3: Four things to mitigate security vulnerability:*Four things an IT manager can do to mitigate security vulnerabilities in cloud based e-learning.Intel recommends prioritizing security investment through a risk assessment to determine the order and timing for building this level of trust and compliance into cloud ecosystem in four areas as follows:

- Encrypt to protect data that rests or moves in the cloudespecially in public clouds.
- Establish a trusted foundation to secure educational institution data center platform and infrastructure and protect clients.
- Build higher assurance into compliance to streamline auditing.
- Establish and verify identities before educational institution federate by controlling access from trusted cloud users in e-learning and trusted systems.

*4) Step 4: Protect data:*Protect data in motion, in process and at rest. Encrypt the data wherever it is in the cloud: at rest, in process, or in motion. Since, data doesn't stay in one place on any network and this is especially true in case of data in the cloud based e-learning.

*5) Step 5: Secured platform:*Securing both client and server platforms in cloud based e-learning are very important as there is increasetrend in malware threats. It will facilitate the additional enforcement point which builds trust between servers and between servers and clients. The best to start is with a trusted hardware based root and extend the chain through the critical controlling software layers.

*6) Step 6: Extend trust across federated clouds:*Additional layer of complexity to the current security equation should be added in cloud based e-learning as it evolves the vision of federated cloud relationships across several cloud infrastructure. Managing identities and access-management policies including standards-based single sign-in (SSO), strong authentication, account provisioning, API security and audit capability can built the trusted access to the cloud and across clouds. Simple usernames and passwords are not adequate for cloud security since it can be easily compromised.In federated cloud environment, strong second-factor authentication is essential for secure SSO.

*7) Step 7: Choose the right cloud service provider:*Choosing the right cloud service provider is tedious process as it involves many levels from the cloud delivery model and architecture to specific applications. In addition to that the countless interdependencies and relationships are exists among the vendors both in terms of technological and business-related.Cloud users in e-learning needs to know about the data and platform protections for the services they offered.

C. Microsoft :Four Checklist for Cloud Security[17]

Microsoft has given the checklist for IT managers to ensure the security in cloud based e-learning as follows:

1) Integration : Integration points needs to be checked with the security and identity management technologies currently available in the educational institution such as active directory, controls for role-based access and entity-level applications.

*2) Privacy:*Educational institution should make sure that cloud service includes data encryption, effective data anonymization and mobile location privacy.

*3) Access:*Educational institutions should aware of the means of preventing inadvertent access when the resources are placed in a shared cloud infrastructure. Cloud Provider's policy on accidental release of protected data must be carefully read by the educational institutions.

4) Jurisdiction: The location of a cloud provider's operation can affect the privacy laws that apply to the data it hosts. Educational institutions need to check the data whether it is to be reside within their legal jurisdiction.

VI. CONCLUSION

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

REFERENCES

[1] D.Kasi Viswanath, S.Kusuma and Saroj Kumar Gupta, "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.

[2] Md. Anwar Hossain Masud, Xiaodi Huang, "An E-learning System Architecture based on Cloud Computing" ,*World Academy of Science, Engineering and Technology 62 2012* available at http://www.waset.org/journals/waset/v62/v62-15.pdf

[3] Paul POCATILU, “Cloud Computing Benefits for E-learning Solutions”, *Oeconomics of Knowledge*, Vol. 2, Issue 1, 1Q 2010.

[4] A. Fern´andez, D. Peralta, F. Herrera2, and J.M. Ben´ıtez,“An Overview of E-Learning in Cloud Computing”,Available:http://sci2s.ugr.es/publications/ficheros/2012-LTEC-Fernandez-E-Learning_CC.pdf

[5] Cloud Computing,[Online] Available:http://en.wikipedia.org/wiki/Cloud_computing accessed on November 2012.

[6] Ajith Singh. N, M. Hemalatha,“Cloud Computing for Academic Environment”,*International Journal of Information and Communication Technology Research*,Vol. 2 No. 2, Feb. 2012.Available:http://esjournals.org/journaloftechnology/archive/vol2no2/vol2no2_1.pdf

[7] http://www.serverschool.com/cloud-computing/why-cloud-computing-will-continue-to-become-popular/ accessed on November2012.

[8] Bhruthari G. Pund*,Prajakta P. Deshmukh, “Appliance of Cloud Computing on E-Learning” *International Journal of Computer Science and Management Research*, Vol. 1 Issue 2 Sep.2012. Available :http://www.ijcsmr.org/vol1issue2/paper43.pdf

[9] Ivan I Ivanov,“Cloud Computing in Education: The Intersection of Challenges and Opportunities” Available: http://www.webist.org/Documents/Previous_Invited_Speakers/2011/WEBIST2011_Ivanov.pdf

[10] Ahmed E. Youssef,“Exploring Cloud Computing Services and Applications”,*Journal of Emerging Trends in Computing and Information Sciences,*Vol. 3, No. 6, July 2012. Available :http://cisjournal.org/journalofcomputing/archive/vol3no6/vol3no6_4.pdf

[11] http://cloud-basedlms-etec522.weebly.com/security.html accessed on November 2012.

[12] 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.087 – 090, Available: http://ijaest.iserp.org/archieves/15-Jul-15-31-11/Vol-No.9-Issue-No.1/16.IJAEST-Vol-No-9-Issue-No-1-Seven-Deadly-Threats-and-Vulnerabilities-in-Cloud-Computing-087-090.pdf

[13] http://www.cloudstandardscustomercouncil.org/Security_for_Cloud_Computing-Final_080912.pdf accessed on December 2012.

[14] http://www.simplysecurity.com/2012/12/04/10-steps-to-securing-your-journey-to-the-cloud/ accessed on December 2012.

[15] http://www.intel.com/content/dam/www/public/us/en/documents/guides/cloud-computing-security-planning-guide2.pdf accessed on December 2012.

[16] http://cloud-basedlms-etec522.weebly.com/security.html accessed on December 2012.

[17] http://www.aicte-india.org/downloads/CloudComputinginEducation.pdf accessed on December 2012.