The Impact of Cloud Computing Technologies in E-learning

http://dx.doi.org/10.3991/ijet.v8iS1.2344

Hosam F. El-Sofany[1], Abdulelah Al Tayeb[1], Khalid Alghatani[1] and Samir A. El-Seoud[2]

[1] Arab East Colleges for Graduate Studies, Riyadh, Kingdom of Saudi Arabia
[2] British University in Egypt (BUE), Cairo, Egypt

***Abstract*—Cloud computing is a new computing model which is based on the grid computing, distributed computing, parallel computing and virtualization technologies define the shape of a new technology. It is the core technology of the next generation of network computing platform, especially in the field of education, cloud computing is the basic environment and platform of the future E-learning. It provides secure data storage, convenient internet services and strong computing power. This article mainly focuses on the research of the application of cloud computing in E-learning environment. The research study shows that the cloud platform is valued for both students and instructors to achieve the course objective. The paper presents the nature, benefits and cloud computing services, as a platform for e-learning environment.**

***Index Terms*—Cloud Computing, E-learning, Learning Actor, architecture of Cloud Education, Secure E-Learning**

I. INTRODUCTION

A. *Cloud Computing Basic Knowledge*

Cloud Computing is a new model for hosting resources and provisioning of services to the consumers. It provides a convenient, on-demand access to a centralized shared pool of computing resources that can be deployed by a minimal management overhead and with a great efficiency. The term "Cloud Computing" sprang from the common practice of depicting the Internet in pictorial diagrams as a cloud Internet. Cloud Computing providers depend on the Internet as the intermediary communications medium leveraged to deliver their IT resources to their consumers on a pay-as-you-go basis. By using cloud computing consumers can be access resources directly through the internet, from anywhere by using any internet devices, and at any time without any technical or physical concerns [1]. NIST (National Institute of Standards and Technology) defines, Cloud Computing is on-demand access to a shared pool of computing resources. It is an all-inclusive solution in which all computing resources (hardware, software, networking, storage, and so on) are provided rapidly to the consumers [8].

B. *The need of society*

The characteristics of cloud computing includes: *virtual*, *scalable*, *reliable*, *efficient*, and *flexible*. Relatively to inexpensive mobile devices and its modern networks, as a fact, computation is increasingly. All Computers that the cloud represents need to scale to this need very quickly. Immediate and automated leasing is a favorite scheduling strategy, since cloud computing is an on-demand computing paradigm. Most of the strategies is both being an automated scheduling and considering the maximum usage of resources. To achieve an optimal or suboptimal allocation for immediate cloud services, the cloud environment with security is the best option [2]. Moreover, it is characterized by:

- A distributed system where applications are stored in a cloud of decentralized servers that can be reached through an Internet connection and a Web browser.
- A strong extensibility at the applications, platforms and infrastructures levels.
- The resources offered by the cloud can be dynamically assigned according to the need.
- A strong tolerance when one or several resources breakdown.
- A business models where customers pay according to the resources used.

Cloud computing is cheaper than other computing models; zero maintenance cost is involved since the service provider is responsible for the availability of services and clients are free from maintenance and management problems of the resource machines, so organizations do not need to pay for and look after their internal IT solutions [1].

C. *Cloud Computing Basic Concept*

The cloud computing is considered as the 5th generation of architecture in the IT world. It follows-up the following architectures in the chronological order of their appearance: Mainframes (1970), Client-server (1980), Web (1990), SOA (2000) and Cloud (2010). In the literature, there are several definitions of the cloud computing that are more or less vague. However, the definition given by the NIST - *National Institute of Standards and Technology* [3] is an authoritative one. The view of the NIST is that the cloud computing has three service models, four deployment models and five essential characteristics as shown in Figure 1[4].

Three widely referenced service models have evolved [5]:

- **Software-as-a-Service (SaaS):** Only hosted applications are provisioned. By using this model you can reduce the cost of hardware and the software development, maintenance and operations.
- **Platform-as-a-Service (PaaS):** In this model, the customer can develop his application on the provider-supported platform. By using this model you can reduce the cost and full management complexity. The

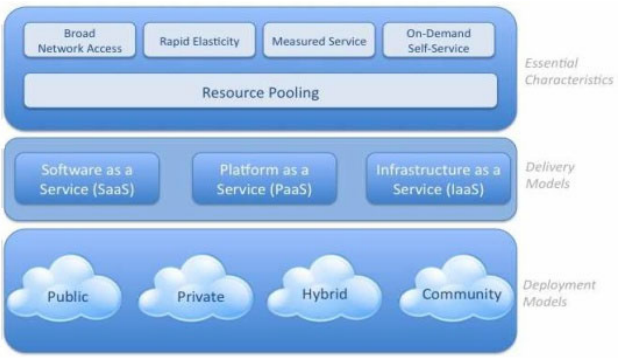

Figure 1. NIST Visual Model of Cloud Computing Definition

customer can manage his required software components of the platform. The development environment is determined by the cloud provider. The cloud customer has control over applications and application environment settings of the platform.

- **Infrastructure-as-a-Service (IaaS):** The Provider hosts the consumer's virtual machines and provides networks and storage. By using this module the customer avoids purchasing and managing the hardware and software infrastructure components, and is provided with all resources virtualized through a service interface.

In addition to these service models, four deployments have been added:

- **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Private cloud:** The cloud infrastructure is accessible for an organization only. It may be managed by the organization itself or a third party and can be internal or external.
- **Community cloud:** A private cloud that is shared by several customers with similar security concerns and the same data and applications sensitivity.
- **Hybrid cloud:** It merges more than one Cloud Computing model into a single, hybrid model; using a public cloud for hosting sites that must be published publically and containing uncritical data, and using a private cloud for all the other sensitive data or services. This scenario is good for economic and business requirements.

In addition to the NIST definition, we can find other service models such as:

- **Hardware as a Service (HaaS):** contrarily to the SaaS and PaaS that provide applications and services to the customers, HaaS offers only the hardware.
- **Database as a Service (DaaS):** the aim of a DaaS is to offer a database and the services allowing its management to avoid the complexity and running cost of a database if hosted in the own network of a company or organization.

Monitoring, addressing security and privacy issues remain in the purview of the organization, just as other important issues, such as performance, availability, and recovery [7].

D. Issues and Challenges

Although the benefits that Cloud Computing offers, there are numerous issues and challenges for organizations embracing this new paradigm. A list number of major challenges with respect to the following:

- Data management and governance.
- Service management and governance.
- Product and process control and monitoring.
- Infrastructure and system reliability and availability
- Information and visualization security.
- Concerns over security with respect to knowledge, information and data residing on an external service device.
- Concerns over services' and resources' availability and business continuity.
- Concerns over data transmission across anticipated broadband speeds.

Other shortcomings include no native security attributes, inadequate or no security provisioning by providers, lack of understanding of Cloud legal issues, and the failure to recognize potential liability from either legal issues or because of lack of security. Issues with respect to "control" are also real concerns [8].

E. Cloud Service Provider CSP Experiment

During these last years, the new cloud computing paradigm has been generalized in the IT world. Actually, the idea of cloud computing is not new as John McCarthy suggested its first enunciation in 1960: "computation may someday be organized as a public utility". This paradigm has been used by Amazon since 2002, where it started to resell its storage and treatment capacities as they were higher than its needs. Nowadays, we can distinguish two main kinds of actors: those coming from the Web as Amazon, Salesforce.com, Google and those coming from the IT as IBM, Microsoft, Sun, HP and Oracle. These actors offer several layers in the cloud to allow the development and online publishing of applications (e.g. the Force.com development platform of Salesforce.com or the Gmail application of Google). Actually, we can find a taxonomy of the existing services offered in the context of the cloud computing [7].

Because cloud service providers (CSPs) are separate administrative entities, moving to the commercial public cloud deprives users of direct control over the systems that manage their data and applications. Even if CSPs' infrastructure and management capabilities are much more powerful and reliable than those of personal computing devices because users don't have access to the cloud's internal operational details, CSPs might also voluntarily examine users' data for various reasons without detection. Additionally, owing to hardware virtualization, multiple users can now share the same physical infrastructure, which runs their distinct application instances simultaneously [6].

II. THE IMPACT OF CLOUD COMPUTING IN E-LEARING

A. E-learning Environment

E-learning environment appears after learning environment impacted by network technology. As a new type of

learning environment, it is causing people's popular attention. There is a various way of expressing it, such as web-learning environment, virtual learning, E-learning environment, digital learning environment and so on. E-learning environment is defined by USA information technology website as: "*E-learning environment is a series of teaching and learning tool, and the learning experience of strengthening students' E-learning and computer's learning in their learning process*". In this, we simply mean to the E-learning environment which mainly take advantages of computers [9].

A good E-learning environment is made up of several functional modules. In [9] the authors hold the views that the construction of E-learning environment should include independent learning tools module, collaborative learning platform modules, FAQ module, resources management module, and E-learning evaluation module five functional modules. This essay only based on the collaborative learning platform module to study the application of cloud computing in education [9].

B. The Advantages of Apply E-Learing in Cloud Computing Environment

Cloud computing construct a free and extensive space, when applied to teaching, we have to ensure that learners' autonomy, but also to improve the effectiveness of learning. Constructing a good cloud computing educational environment, will help to make full use of educational accessibility of cloud computing, to take advantage of cloud computing for more effective learning of learners [9].

The benefits of "software as services" in schools may be described by several factors. The first, it provides a solution to the problem of licensed software that requires constant updating. The second is that the learning process requires searching and experimentation. A flexibility, provided by cloud technologies, enables to modify, test and compare different types of software, various forms of use that would be impossible if purchase every time new software and equipment and support them [10]. The third is multiply access to large data collections possibility [11].

- **CaaS (Communication as a Service)** is a new service that is derived from SaaS. Communication aids, for example, e-mail is used as a service that can be provided to the entire school (students, teachers, administration). Along with this the significant amount of virtual space where students can, if necessary, store large media or image files is given. Another advantage of this service is that students can use email remotely in any city, by mobile devices [10, 11].
- **DaaS (Desktop as a Service**) is a technology where users receive a completely ready virtual workplace as a service. This technology is derived from SaaS, it is spread in recent years. A learner gets access to an environment that may be further customized according to his needs and goals. The advantage of this technology is that hardware requirements are minimal and it allows reducing costs significantly. The customer pays exactly for what he (she) needs and if necessary. Thus, it appears a possibility to provide considerable amount of academic content by very cheap hardware [10, 11].

III. E- LEARNING ARCHITECTURE BASE ON CLOUD ENVIRONMENT

A. Constructing a Distributed Service System of Distance Education Resources

Cloud computing can connect different geographical distribution of resources including computers, databases, storage devices, into a relatively transparent to the user's high-performance virtual computing environment. User can access to resources through education interface. They can also access to a existing resource management system for all teaching resources database services, and can get new teaching resource data from the repository see Table I. [12].

TABLE I.
DISTANCE EDUCATION INFRASTRUCTURE BASED ON CLOUD COMPUTING SERVICES

Layer	Resources
L5	Student / Teacher
L4	Distance Education Application
L3	Cloud service interface
L2	Distance Education platform services based on cloud computing
L1	Distance Education Resource Database Computers Switches Routers

The second layer (L2) is distance education cloud computing platform service. It is critical to achieve services, because this layer is transparent to students or teachers. They needn't to know the details of the layer. They needn't to know how the cloud services are implemented. For the layer which services are implemented, and how to provide services outside, these are released by the third layer (L3), so called Cloud service interface. For students or teachers (L5), they need only enjoy the cloud services through distance education applications (L4) [12].

B. Learning Actors in Cloud Computing

A Learning Actor is any entity involved in the learning process like management, students, instructors, lab staff etc.

There are four types of resources that can be provisioned and a Learning Actor can consume over the Internet [13].

- Infrastructure resources including computing power, storage, and machine provisioning.
- Software resources including middleware (cloud-centric operating systems, application servers, databases) and development resources (development, testing tools, and deployment tools).
- Application resources. Educational Software applications are delivered through Software As A Service (SaaS) model or mashups of value-added applications.
- Learning processes. Applications exposed as utilities or tasks. Learning process sharing is the learning-driven application outsourcing that supports provisioning, reuse and composition.

Cloud Learning Objects and Cloud Learning Processes will be greatly benefited by the following two key technologies that will play very important roles in this revolu-

tionary phase: virtualization technology and Service-Oriented Architecture (SOA) [13],[14].

- The virtualization technology manages:
  - The imaging of the operating systems, middleware, and applications.
  - The pre-allocation of all the resources to the right physical machines or server stack slices; ideally, images should be moved around and put into production environment on demand.
  - The licensing mechanism of all software layers in the cloud computing platform.
- The SOA supports component-based software development improving reusability, extensibility, and flexibility.

In order to construct scalable cloud computing platforms, we need to leverage SOA to build reusable components, standard-based interfaces, and extensible solution architectures.

Creating a cloud computing platform is crucial in enabling sharing and reusing of its resources. The idea is when new learning objects are needed we should be able to consume (reuse with the least effort) existing resources and assemble new courses running on a Unified Cloud Computing Educational infrastructure [14].

C. An architecture based on Cloud Computing with the Name "Cloud Education"

The model contains physical hardware layer, virtualization layer, education middleware layer, application program interface layer, management system and security certification system see Figure 2.

- **Physical hardware layer** is a basic platform in model, including servers, storage equipments, and network equipments.
- **Virtualization layer** with the feature: dynamic configuration, distributed deployment, fee measurement realizes the five characteristics of cloud computing. The goal of virtualization layer is to break completely information islands based on existing regional through the distributed technology and virtualization technology. This layer also consists of three parts: virtual servers, virtual storages, and virtual databases [15].

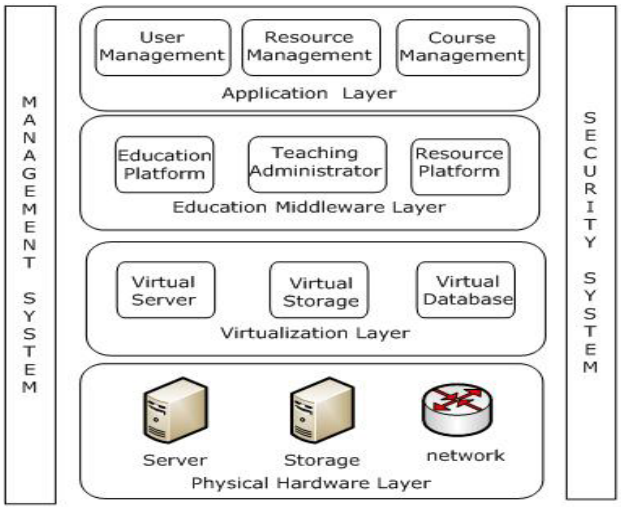

Figure 2. Architecture of Cloud Education model

- **Education middleware layer** is the core layer, because it is the basic business platform. This layer is different from existing, and all information attached to it on different computing node including ordinary file and database. So, all application systems on the middleware layer have
- **Application program interface layer** can guarantee model's scalability. Because of the diversity of the existing application system and an application system cannot satisfy all the needs of customers. In this layer also provide the necessary interface beside, and still need to be able to provide hosting service.
- **Management system** mainly watchers physical condition, virtualization software, hardware and software, open API. Management system can enhance the safety of the software platform.
- **Security system** includes identity authentication and authorization, single point login, virtualization software and hardware access control and audit, the education middleware and open API access control [16].

IV. PRIVACY AND SECURITY IN E-LEARING

Security and privacy problems appear in e-learning because of operation mechanism and policy mechanism. The failure of security technology makes personal privacy be spread, diffused, aggrieved and scouted without permission. Loopholes in the law led to the network managers could store, amend, exchange, and sell personal information without punishment. In this paper, we classify the privacy violation phenomenon of e-learning process during the information to be collected, used, saved, and deleted and so on.

A. E-learning Security issues

Some of the most serious threats are listed below [19]:

- Deliberate software attacks (viruses, worms, macros, denial of service)
- Technical and human failures and errors (bugs, coding problems, accidents)
- Deliberate acts of espionage or trespass (unauthorized access and/or data collection)
- Deliberate acts of sabotage or vandalism (destruction of information or system)
- Technical hardware failures or errors (equipment failure)
- Deliberate acts of theft (illegal confiscation of equipment or information)
- Quality of Service deviations from service providers (power and WAN service issues).

The primary concern in E-Learning is the security that can be summarized as following [18]:

1) *User Authorization and Authentication*

The elementary feature of E-Learning system is the reliable identification – recognition of the user as a genuine member of a user community because it is the basis for Access control to the E-Learning system. *Authentication* – verification of the user's identity. *Authorization* – permission to access specific resources. The Authorization is usually is granted only to registered students and even their access is generally restricted to a certain subset of the E-Learning material based on the billing if E-Learning is

offered on billing basis and on the level of learning of the registered student which will allow him to either to move to the next level or have a revision of the previous session.

2) *Entry Points*

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

3) *Dynamic Nature*

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

4) *Protection Against Manipulation*

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

5) *Confidentiality*

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

6) *Integrity*

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

7) *Availablity*

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

8) *Non-Repudiation*

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

B. Counter Measures to Security Attacks

Some of the possible mechanisms that can be applied counter the security threats are:

1) *SMS (Short Message Service) Information Security Mechanism*

Most of the students have a mobile phone as a means of communication, this can be an added advantage to the universities offering E-Learning system, where a student is first authenticated with a user id and password, the E-Learning system generates a special password for the session and sends SMS message to the registered mobile phone in the E-Learning system.

2) *Biometrics Information Security Mechanisms*

Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. According to which all the students are required to enroll their physical or behavioral traits, which is stored in the database which is encrypted from any modifications.

3) *Token Based Information Security Mechanisms*

A security token called sometimes as hardware token, hard token, authentication token, USB token, cryptographic token, or key fob may be a physical device that an authorized user of computer services is given to ease authentication.

4) *Access Control List (ACL) Mechanism*

Access control list provides the access to the resources found in the system or the web server. Any access control will have two components for successful functioning of the system. In an E-Learning environment the student has to have access to the resources they are intended for there are configuration tools that allows to grants which user have access to which resources and a means to authenticate the users to identify them properly, which can be controlled by using the one of the three most popular methods for authenticating and controlling access to the users in a web scenario. They are the host based access control, basic authentication, and access through SSL / TLS client certificates.

5) *Digital Signature Information Security Mechanisms*

Digital Signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact this feature can be easily applied to E-Learning system and any changes to the documents can be verified whether the intended user has tried to make any modifications to the e-content.

6) *Security from Passive Attacks*

The measures discussed above can be used to detect the Active attacks, the Passive attacks can be prevented by adopting cryptographic algorithms on the basis of security and performance requirements of e-contents so that the users can't understand the message, Cipher and authentication are two important concepts in cryptography. By cipher, the eavesdropping can be avoided and confidentiality which is the inverse concept of eavesdropping can be achieved. Cryptography can be used for user authentication. Generally three types of cryptographic schemes are used to accomplish these goals: Secret Key or Symmetric Key Cryptography, Public Key or Asymmetric Key Cryptography and Hash Functions [18].

C. *Secure E-Learning Platform Based on SOA-Based Architicture*

A secured e-learning platform takes advantage of the design of distributed and loosely-computational services. Building the platform on a service architectural style provides a model in which functionality is decomposed into distinct computational units or services, which can be distributed over local or remote networks and can be combined together and reused to create secured applications. These services exchange with each other by passing data from one service to another, or by coordinating scenarios of security access between two or more services. The flexible, standardized architecture can be seen as a distributed security system that provides various access services for a wide range of devices. This security service system supports the development of various e-learning applications that require security access services, which can be remotely invoked to grant or deny the access of tutors, students and administrators. As shown in Figure 3, the platform comprises the following components:

1) *Profile/Role/Rights/Context Management (PRRC)*

allows the authorization manager to create a set of defined Profiles of users (i.e. students, tutors,) or things (i.e. courses, transcripts, …) and assigns them different Roles that allow them appropriate rights (i.e. read files, access a room, turn on machines, …) to access various Resources (i.e. room, databases, labs, …) based on a specific context (i.e. time, location, environments, …).

The management mainly distinguishes between two categories: human entities and objects (Thing).

2) *Profile/Role/Rights/Context Management (PRRC)*

allows the authorization manager to create a set of defined Profiles of users (i.e. students, tutors,) or things (i.e. courses, transcripts, …) and assigns them different Roles that allow them appropriate rights (i.e. read files, access a room, turn on machines, …) to access various Resources (i.e. room, databases, labs, …) based on a specific context (i.e. time, location, environments, …). The management mainly distinguishes between two categories: human entities and objects (Thing).

3) *Input Devices*

Denote a set of input peripherals used to acquire access requests from Humans or Things. Input devices constitute a ubiquitous environment to recognize several types of security accesses within specific contexts. Input devices acquire and transfer the security requests in the form of multimedia-based access requests. A rough list of input devices may include: Sensors, Camera, Videos, Voice Recorder, Motion / Shape Detectors, IP address.

4) *Context-Aware Access Services (CAS)*

Constitute the core of the platform and are built in terms of services that provide various security accesses according to multimedia-based requests. These services are published as web services and can be remotely invoked by input devices (or applications) to process request access to resources. This component is extensible, open and standard-based which guarantees the appropriate evolution of the platform and independence from input devices. In addition, the development of this component is considered as a distributed security system that provides various access services for n-tier applications.

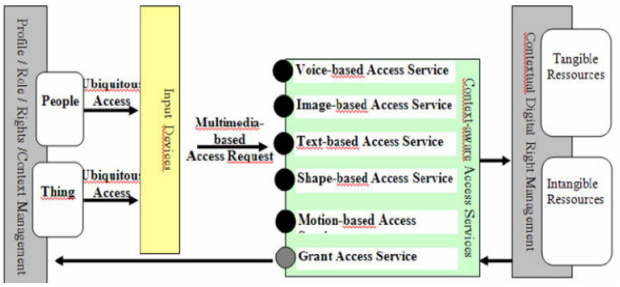

Figure 3. Security Architecture for e-learning SOA- based Architecture

5) *Contextual Digital Right Management (CDRM)*

Aims to add additional levels of security by assigning rights to owner of resources. The Management of Digital Rights provides access control technologies to use by resources holders to limit usage of digital media or devices. It also refers to restrictions associated with specific instances of digital resources. The use of contextual digital rights management (CDRM) provides advantages to decouple the access to Resources from the access rights assigned by PRRC management. The context of resources is taken into account to grant access to authorized input objects according to contextual predicates.

6) *Resources*

Presented by two types; Tangible resources such as Things (e.g., products) or Space (e.g., room, lab) and Intangible resources such as time (e.g., processor time), digital works (e.g., text file, patents, music, vide) [17].

ACKNOWLEDGMENT

The authors acknowledge the full support received from Al Arab East Colleges for Graduate Studies, especially they very thankful to Professor Dr. Abd Allah Al Faisal, Dean of the Colleges, for his encouragement and support.

REFERENCES

[1] Engr: FarhanBashir,Mr.SajjadHaider 6th International: Conference on Internet Technology and Secured Transactions, 11-14 December 2011, UAE.

[2] PriteshJain,DheerajRane and ShyamPatidar: A Survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment, 978-1-4673-0126-8/11/$26.00_c 2011 IEEE

[3] P.Mell, T. Grance.: NIST definition of cloud computing. National Institute of Standards and Technology. October 7, 2009.

[4] Christian Delettre*, KarimaBoudaoud , Michel Riveill: Cloud Computing, Security and Data Concealment978-1-4577-0681-3/11/$26.00 ©2011 IEEE

[5] Wayne A. Jansen: Cloud Hooks: Security and Privacy Issues in Cloud Computing NIST Proceedings of the 44th Hawaii International Conference on System Sciences – 2011

[6] T. Ristenpart et al.: "Hey, You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS 09), ACM Press, 2009, pp. 199–212.

[7] Open Crowd. Cloud Taxonomy, Landscape, Evolution. http://www.opencrowd.com/assets/images/views/views_cloud-taxlrg. png. June 8, 2010.

[8] ZaighamMahmood, Richard Hill: Cloud Computing for Enterprise Architectures (Book).

[9] Hui Ma1 ZhongmeiZheng, Fei Ye and Sanhong Tong: The Applied Research of Cloud Computing in the Construction of Collaborative Learning Platform under E-learning Environment: 978-0-7695-4223-2/10 $26.00 © 2010 IEEE

[10] N. Sultan: "Cloud Computing for Education: A New Dawn,International Journal of Information Management, n.30, pp. 109–116.,2010. http://dx.doi.org/10.1016/j.ijinfomgt.2009.09.004

[11] ShyshkinaMariya: Cloud computing – an advanced e-learning platform of school education, 978 -1-4577-1747-5/11/$26.00 ©2011 IEEE

[12] HongyuZhao, Yongqiang Wang, Liyou Yang: Research on Distance Education Based on Cloud Computing: 978-1-4577-0208-2/11/$26.00 ©2011 IEEE

[13] L. Zhang and Q. Zhou, "CCOA: Cloud Computing Open Architecture", IEEE international Conference on Web Services 2009, IEEE Computer Society, pp. 607-616.

[14] PanagiotisKalagiakos, PanagiotisKarampelasCloud Computing Learning: 978-1·61284·832-7/11/$26.00 ©2011 IEEE

[15] Wang, L.Z., G. von Laszewski, D. Chen, et al. Provide Virtual Machine Information for Grid Computing[J]. Ieee Transactions on Systems Man and Cybernetics Part a-Systems and Humans, 2010,40(6): 1362-1374. http://dx.doi.org/10.1109/TSMCA.2010.2052598

[16] Research on the Architecture of Open Education Based on Cloud Computing Xiaojun Wang , Daohua Huang 978-1- 61284-704-7/11/$26.00 ©2011IEEE

[17] Pascal Bou Nassar, Youakim Badr: Towards Integrating Security Services in e-learning Platforms; Kablan Barbar, Frédérique Biennier978-1-4244-3834-1/09/$25.00 © 2009 IEEE

[18] Shakeel Ahmed, Khalid Buragga , Ashwani Kumar Ramani: Security Issues Concern for E-Learning by Saudi Universities; ISBN 978-89-5519-155-4 Feb. 13~16, 2011 ICACT2011

[19] Najwa Hayaati Mohd Alwi, Ip-Shing Fan: E-Learning and Information Security Management; International Journal of Digital Society (IJDS), Volume 1, Issue 2, June 2010

AUTHORS

Hosam F. El-Sofany is with Department of Computer Science**,** Arab East Colleges for Graduate Studies Riyadh, Kingdom of Saudi Arabia. (hosam_elsofany@hotmail.com)

Abdulelah Al Tayeb is with Department of Computer Science, Arab East Colleges for Graduate Studies**,** Riyadh, Kingdom of Saudi Arabia. **(**atayeb@gmail.com)

Khalid Alghatani is with Department of Computer Science, Arab East Colleges for Graduate Studies, Riyadh, Kingdom of Saudi Arabia. (kalghatani@yahoo.com)

Samir A. El-Seoud is with Faculty of Informatics and Computer Science, British University in Egypt-BUE, Cairo, Egypt. (Samir.elseoud@bue.edu.eg)

This article is an extended and modified version of a paper presented at the International Conference on Interactive Collaborative Learning (ICL2012), held 26 - 28 September 2012, in Villach, Austria. Received 6 November 2012. Published as resubmitted by the authors 3 December 2012.