I.J. Information Technology and Computer Science, **2018, 4, 1-9**
Published Online April 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2018.04.01

E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure

Olugbenga W. Adejo
University of the West of Scotland, Paisley, United Kingdom
E-mail: olugbenga.adejo@uws.ac.uk

Isaiah Ewuzie, Abel Usoro and Thomas Connolly
University of the West of Scotland, Paisley, United Kingdom
E-mail: {Isaiah.ewuzie, abel. usoro, thomas.connolly}@uws.ac.uk

Received: 12 November 2017; Accepted: 29 January 2018; Published: 08 April 2018

***Abstract*—**In recent years, the advancement in internet technologies has greatly altered the learning landscape, thus, a shift from traditional methods of learning to internet based learning platforms. E-learning, m-learning and cloud are some of the most powerful responses to these growing technological shift by the education sectors. Their impact and benefits cannot be over-emphasized with regard to making learning accessible, affordable, available and convenient. In addition, the use of cloud technology has made the world of education more integrated, networked and composite. This makes e-learning and m-learning as highly effective as the conventional method of learning delivery. However, despite these advantages, the security and the protection of learners’ data on this cloud platform have been some of the major challenges to m-learning effective implementation and use.

This paper discusses the various benefits of the using m-learning platform and cloud infrastructure in higher education. It also examines the vulnerabilities of the platform as well as other security and privacy challenges regarding the effective implementation of m-learning in cloud infrastructure environment. Finally, it proposes a detailed data protection and security framework that is needed for addressing these issues. It is expected that the proposed framework when fully implemented, will bring about necessary solution to issues relating to the security and data protection of m-learners in cloud computing environment, increase trust in the use of the system as well as enhance the m-learning platforms.

***Index Terms*—**Electronic learning, Mobile Learning, Learning Analytics, Cloud Computing, Security Framework.

I. Introduction

E-learning emerged from the traditional/classroom learning in the late eighties and nineties leveraging the power of ICT and computing. The emergence of e-learning has altered the educational landscape by creating new learning possibilities for people from all works of life. E-learning has made education universally available, more affordable and convenient, thus, the unprecedented increase in the online colleges, universities and training centres. The use of ICT and the internet in learning gives e-learning edge over traditional classroom methods. However, due to deficiencies of the e-learning in the areas of cost and time disadvantages as well as the advancement in Internet technologies (leading to emergence of cloud computing), the world is witnessing a shift in the usage of e-learning to mobile learning (m-learning). Fig. 1 below shows the development trend in learning platform.

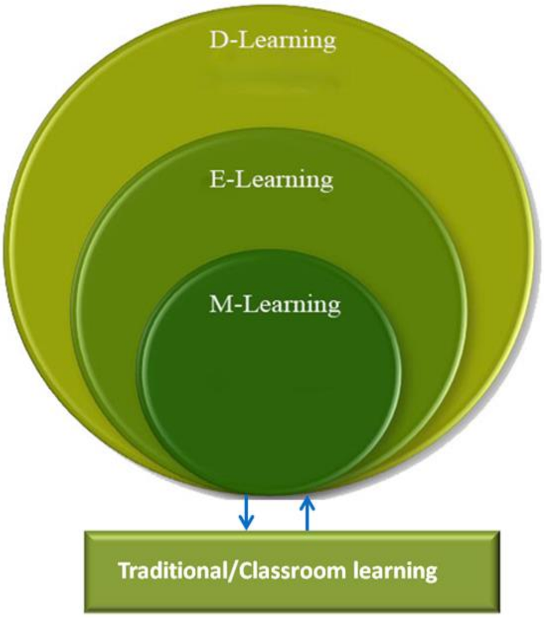

Fig.1. Evolution of learning platforms

In the last few years, there has been a significant development of mobile technology from the simple cell phone to the current high-tech smart phones and tablets. Every sector, banking, commerce, health, security and education have not been left behind in the use of this new technology as we moved to the era of not just online but, mobile communication. M-learning is a term that denotes the delivery of learning materials and other content through the use of mobile devices that can easily be accessed anywhere in the world [1] and at present many further and higher educational institutions are using it.

The term mobile learning refers to learning activities that can take place in multiple locations and at any time with various types of small portable devices such as smartphones, laptops, netbooks, tablets, personal digital assistants (PDAs), MP3/MP4 and other handheld devices such as video player, PSP, Nintendo [2]. M-learning can be used to access documents or document libraries for quizzes and assignment participation in lesson and tutorial, watch education video and live lecture broadcasts, contribute to forums as well as exhibit student work. Furthermore, countries such as the United Kingdom, Austria, Slovenia, Italy, Greece and Croatia, have incorporated game-based learning to target young audience [3].

A deep look into the operation of the m-learning shows that it naturally emerges from the e-learning method. In fact, there have been several examples of the use of e-learning in m-learning technologies; however, the main advantage of m-learning over e-learning is the unrestricted availability of information irrespective of time and environment [4]. In a study by [4] a tabular comparison of the major differences between e-learning and m-learning was given as shown below in Table 1 and 2.

Table 1. Differences between e-learning and m-learning (Adapted from Korucu et al., 2011)

e-learning	m-learning
Computer	Mobile
Bandwidth	GPRS, G3, Bluetooth
Multimedia	Objects
Interactive	Spontaneous
Hyperlinked	Connected
Collaborative	Networked
Media-rich	Lightweight
Distance learning	Situated learning
More formal	Informal
Simulated situation	Realistic situation
Hyperlearning	Constructivism, situationism, collaborative

Table 2. Differences between e-learning and m-learning (Adapted from Korucu et al., 2011)

	E-learning	**M-Learning**
Aim	For in-depth knowledge about a subject	Quick accessibility and Knowledge transfer when needed
Approach	Formal learning	More flexible and informal than e-learning. Allow more freedom
Medium	Desktops or Laptops	Mobile devices- Phone, tablet, PDA
Accessibility by user	Limited to where there is internet and static	Anywhere, No geographical boundaries
Design	Detail information and more media interactivity	Sometimes the information may not be detailed but bite-sized modules
Retention	Varied	High due to level of accessibility on the go
Cost	High cost of acquisition of desktop or laptop	Mid-range cost, affordable by many

However, one crucial issue that urgently needs to be addressed as we move deep into m-learning is the security challenge of it use in cloud infrastructure as well as vulnerability of major technologies (mobile devices) as well as the network system to different forms of attack.

This paper however, propose a data protection and security framework for m-learning that can be used within cloud infrastructure with enhance protection cutting across all the three components -the devices, the network and the cloud infrastructure. The rest of the paper presents benefits of m-learning to higher education, cloud computing concepts, the use of cloud computing in HE, challenges and dangers inherent in the use of cloud infrastructures in HE, the proposed data protection and security architecture; and conclusion and areas for further research.

II. Benefits of M-Learning to Higher Education

Mobile learning is being used in support of traditional learning in HE, blended education as well as in distance learning [4]. The benefits of its use are numerous and include

a) Adequate engagement of young learners any place, any time thus, no geographical boundaries.

b) The technology contributes to combating the digital divide as most people have access to phone unlike computer or desktop

c) Portability- the tablet, smartphone, PDA can be easily used and carry anywhere unlike laptop or desktop as such, students can have access to material unrestricted as well as not limited to classroom space and time for learning.

d) Enables collaborative working among student as they can work at the same time on assignment in different locations.
e) It enhances learning effectiveness as well as develops great autonomy among students.

However, for one to enjoy the maximum benefit from the use of m-learning, there must be a good internet connectivity for downloading, uploading and online working, mobile phone with network or wireless network as well as linkage to institutional learning system, for example Learning management system (LMS) or VLE. Other limitations to the use of m-learning include lack of common operating system and common hardware platform for operating system, design challenges (technical features of the device) and evaluation challenges [5]. In addition to all these challenges, the use of cloud infrastructure for the m-learning has created a unique security challenge that must be properly addressed in order to forestall dangers inherent in loss or misuse of learner or institutional data. Research findings indicate that both lecturers and students are interested in adopting m-learning; however, the security issues relating to data loss, privacy loss, privacy infringement as well as trust of the system have been a major hindrance to them [6].

III. Cloud Computing Concepts

The term cloud computing (CC) has been described by many authors differently. It is a new paradigm with new technologies, such as virtualisation [7], [8], [9]). However, CC leverages the power of the internet to provide computing resources – hardware, software, infrastructure, platforms, data, etc – on demand to end users. The National Institute of Standards and Technology, [10] describes CC as a model for enabling convenient, on-demand network access to shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The NIST definition of cloud is widely accepted because it contains the following characteristics:

1) On-demand self-service: Ability of consumers to access computing resources (e.g. server time and network storage) instantaneously and unilaterally without need for human interaction.
2) Broad network access: Computing resources and capabilities are available over the network (e.g. Internet) and accessed using various heterogeneous platforms (e.g., mobile phones, tablets, laptops and workstations).
3) Resource pooling: The ability to pool providers' computing resources to serve multiple consumers using a multi-tenant virtualization model while dynamically meeting the needs of the consumer. With a pool based model the consumer has no control or knowledge of the exact location as the computing resources (storage, processing etc) are virtualized.
4) Rapid elasticity: Ability to provision instantaneously and dynamically based on particular needs and demands at any time.
5) Measured service: Being able to measure usage of computing resources with the use of metering mechanism such that resources are better controlled and monitored.

The table below summarises the key characteristics and concepts by different authors and researchers:

Table 3. Cloud computing key concepts

Authors	Software	Hardware	Service	Data	Scalability	Virtualisation	Network	Pay-Per-Use	SLA	No Upfront Cost
[7]		√			√	√			√	
[8]	√	√	√			√	√			
[9]					√	√	√			
[27]	√	√	√				√			
[10]	√	√	√		√	√	√	√		
[22]	√	√	√				√			
[23]	√	√			√	√		√		√
[24]		√	√		√	√		√	√	
[25]	√	√	√	√						
[26]	√	√	√		√		√			
Total	**7**	**9**	**7**	**1**	**6**	**6**	**6**	**3**	**2**	**1**

CC is classified based on service provided and method of deployment. The three main cloud service models are: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and the recently emerging Data as a Service (DaaS) that delivers virtualised specific data on demand. Cloud deployment models are: private cloud, community cloud, public cloud and hybrid cloud.

IV. The Use of Cloud Infrastructure in HE

The demand for higher education is increasing due to a number of factors e.g. the growths in the world's population. Staff and students mobility are also on the increase due to globalisation. IT however, plays a significant role in ameliorating the pressure on the demand for places in higher institutions and the associated increase in cost [11].

By using internet platforms along with their communication, collaborative and interactive features, CC has become an attractive proposition to organisations and higher educational institutions (HEIs) alike to conduct their businesses. This is because CC overcomes the complexities involved with hardware and software configuration that are commonplace in other platforms. Furthermore, it has the potential to deliver dynamic mobile interactive computational services by exploiting and leveraging on integrated IT infrastructure [19] [20].

HEIs are constantly availing themselves of opportunities to exploit and share teaching capabilities, learning resources and content management through their online presence [11]. [12] went further to classify and summarise various infrastructures for educational institutions in their research. With CC, wider audience are reached with learning contents and learners' choices are personalised to deliver classes synchronously and asynchronously. In addition, CC allows for greater flexibility, enhanced availability and mobility in the use of resources to meet the need of the end users as well as deal with the problem associated with teaching a large group. As such, many higher institutions are moving into cloud adoption and uses in order to achieve operational efficiency, unrestricted application availability as well as economies of scale. The cloud computing deployment for m-learning in HE can be seen through the three service models as shown in the Fig.2 below.

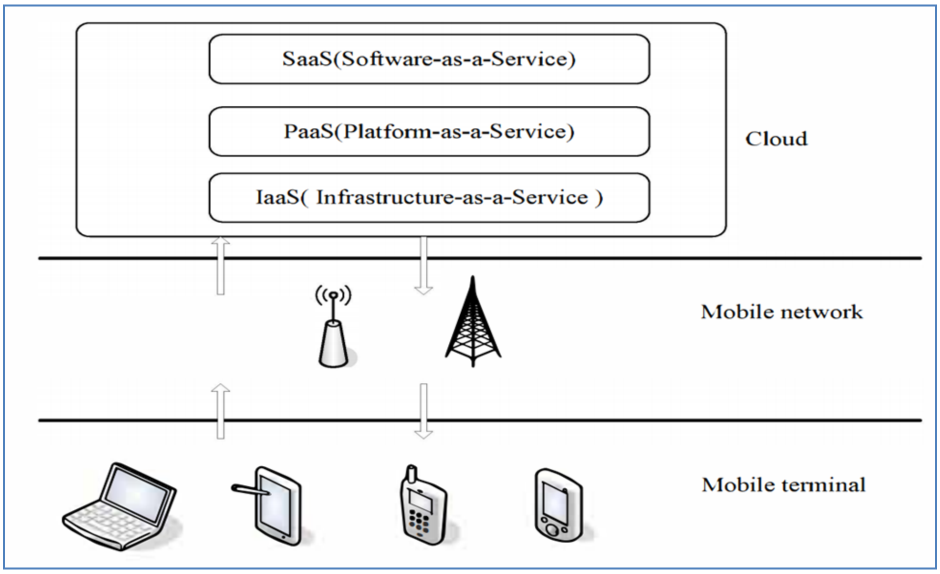
SaaS(Software-as-a-Service)
PaaS(Platform-as-a-Service)
IaaS(Infrastructure-as-a-Service)
Cloud
Mobile network
Mobile terminal

Fig.2. Model of Mobile Cloud computing (Adapted from [28])

1) *Software as a service (SaaS)* - This allows HEIs to use the application and other software through the cloud platform. For example Microsoft (Office 365) Adobe (Creative suite), Odyssey, e-book (Override) and Google apps
2) *Platform as a service (PaaS)* - Help HEIs to use application development environment to design and customized their virtual lab for their learners/ students using PaaS. Examples include Microsoft (Window Azure) and Google (App engine)
3) *Infrastructure as a Service (IaaS)* - This allows HEIs to deploy and run application and other operating software for processing, networking and storage. Examples include Amazon AWS.

V. Challenges and Dangers Inherent in the Use of Cloud Infrastructure

Despite the perceived advantages of CC in higher education, it is not without challenges and inherent dangers. A number of technical challenges will need to be overcome before CC could be fully adopted and used by the HEIs. For instance, CC is multi-disciplinary, thus, requires a good knowledge and skill in virtualization, routing, data use, security etc by the IT and administrative staff most of whom do not have such skills [13].

CC being a new technology poses its challenges as research is still in the infancy stages thus, HEIs will face more than just technical and cost challenges [14]. As [15] pointed out, organisational cultural difficulties and lack of expertise to manage risks and service performance with third parties act as part of the challenges facing HEIs. [16] identified security, performance and availability, compatibility issues, cost associated with vendor integration and management as some of the challenges facing HEIs. [12] summarised challenges and cloud specific issues in relation to education. They went further to classify the various challenges in the use of cloud infrastructures for educational institutions as shown in the table below:

Table 4. Challenges in cloud infrastructure

Cloud Security Issues/ Challenges	Type of Breaches
Top Threats	Data breaches
	Data loss
	Account or service traffic hijacking
	Insecure interfaces and application programme interfaces
	Denial of Service attacks (DoS)
	Malicious insiders
	Abuse of cloud services
	Shared technology vulnerabilities
Policy and Organisational Risks	Lock-in
	Loss of governance
	Compliance challenges
	Cloud service termination or failure
	Supply chain failure
Technical Risks	Isolation failure
	Resource exhaustion
	Intercepting data in transit
	Insecure of ineffective deletion of data
Legal Risks	Issues due to jurisdiction
	Data protection risks
Other Risks	Unauthorised access
	Theft of equipment
	Natural disasters

However, when m-learning is used in cloud infrastructure, the security threats and cyberattack risk to learners and institutional data increase. These attacks have significant impact on the learners, organisations and educational institutions. The fig. below presents a component diagram of the different vulnerabilities from the mobile device to cloud computing infrastructures.

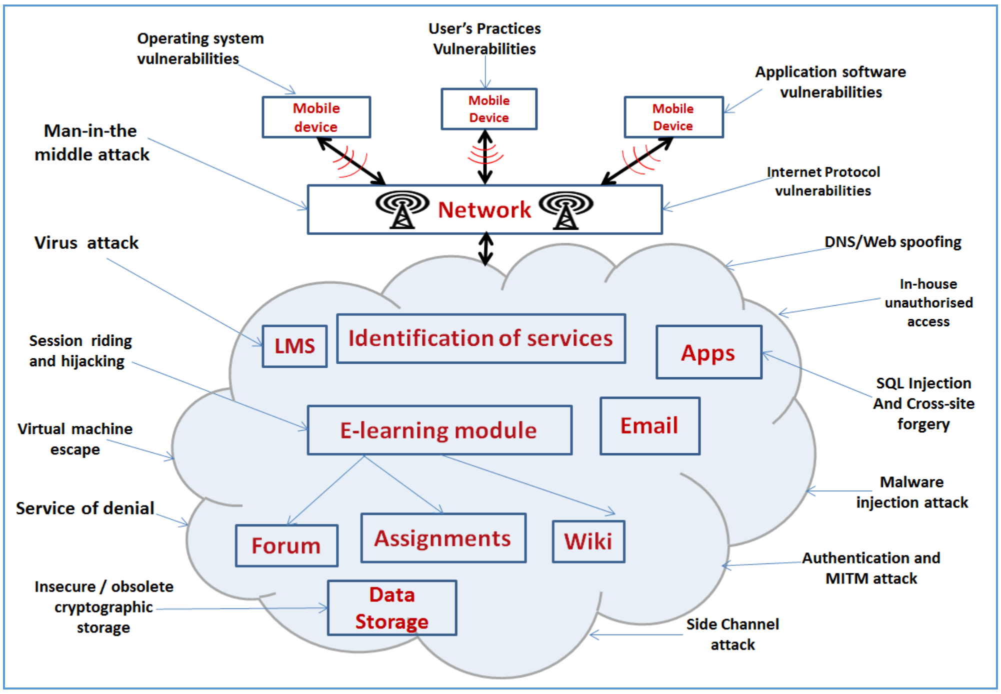
Operating system vulnerabilities
User's Practices Vulnerabilities
Application software vulnerabilities
Mobile device
Mobile Device
Mobile Device
Man-in-the middle attack
Network
Internet Protocol vulnerabilities
Virus attack
DNS/Web spoofing
In-house unauthorised access
LMS
Identification of services
Apps
Session riding and hijacking
SQL Injection And Cross-site forgery
E-learning module
Email
Virtual machine escape
Malware injection attack
Service of denial
Forum
Assignments
Wiki
Authentication and MITM attack
Insecure / obsolete cryptographic storage
Data Storage
Side Channel attack

Fig.3. Cloud vulnerabilities

The mobile devices- This includes the vulnerabilities that most mobile devices such as phones, smart phones, tablet, PDAs are expose to, just like any other computer system. These are operating system vulnerability, mobile web browser security, application based threats such as untrusted application, application collusion, spyware, malware attack, data leak, jailbreak (situation in which the built-in restriction on security is bypassed) as well as other user's personal practices. The threats from the attackers are increasing in sophistication and often happen during downloading and installation of application. When the attacks happened, sensitive information and money of learner or staff can be stolen. Similarly, malicious sms and push advertisement can be sent to others in form of distributed attack. The extent of the attack can lead to the betrayer of the users trust and loyalty on the security and reliability of the mobile devices [1]. However, the system illiterates and security-unaware users often fall for the antics of the attackers.

The network platform (provider) –This is vulnerability inherent in the service provider that the mobile device belongs. The attack may be in the form of the malicious external agent supplanting the server in order to carry out the attack as well as breaking internet protocol.

The Cloud Platform - The cloud infrastructure platform is highly susceptible to malicious attack from outsiders, in-house staff or cloud computing users. This raises high security concerns with respect to cloud physical security, data integrity, encryption/ decryption controls and payment security on the cloud [12]. There are different vulnerabilities that are found in the cloud platform which often lead to attacks such as:

1) **Distributed denial of service (DDOS):** involves the attacker preventing legitimate user from having access to the information or services provided the cloud infrastructure provider and this is done by degrading or completely breaks down the users network connectivity and other network resources (CPU, web server, storage). In most cases, the attacker uses distributed denial of service which includes bandwidth depletion (flooding attack, amplification attack) and resources depletion (malformed packet, protocol vulnerability exploitation).
2) **Malware injection attacks:** involves attempts to inject a malicious service, application or even virtual machine into the cloud system depending on the cloud service models (SaaS, PaaS and IaaS). In order to perform this attack, the attacker exploit the vulnerability of the web application by creating his own malicious web application, service or virtual machine instance and this is added or embedded into the cloud system services. Once the malicious software has been added to the cloud system, the attacker has to trick the cloud system to recognise and treat the malicious software as a valid instance.
3) **Side Channel attack:** involves directing attack to compromise infrastructure as a Service (IaaS) by placing a malicious virtual machine as co-resident to the target cloud server. It mostly targets cryptographic algorithms implementation in the cloud system [17].
4) **Authentication and MITM attack:** involves using a method and process used for authentication of users. Attackers target users where simple username and password combination-type of authentication are used. The authentication method and process might have weakness inherent in them as such might allows credential interception and replay. From this weak point, the attackers can place themselves in the communication path that is, between the user device and service provider in order to carry out attack. This is known as Man-In-the-Middle attack (MITM).
5) **Virtual machine escape:** is a security attack that compromise isolation between VM and the host machine. The program running on the VM is able to bypass the virtual layer so as to get access to the host machine. Once the program has access to the host machine, it can take control and cause complete breakdown of the security architecture of the host through the attack.

The devices- This involves enhancement of the security features, the different software and application in the different mobile devices used by the students, tutors, lecturers and staff This includes using multiple client authentications and multiple firewalls for the mobile web browser and institutional network server. In addition, malware detector can be used to detect malicious malware in the application programing interface (API) and this can be easily to the mobile security tool which becomes effective during mobile device scanning.

Network level: It involves the network reliability such as secure routing, authentication and access control as well as adequate network application security and firewall.

Cloud Platform: solutions to the challenges of cloud computing platform include:

1) *Distributed multi-cloud storage:* involves distributing encrypted sensitive data of the higher institution on the cloud provider multi -cloud storage facilities. This could be a potential solution to the data security issues in cloud as it will help in managing and spreading out the heavy traffic to the cloud infrastructures especially during peak period (load balancing). It could also be used to overcome the problem of maximum-size file.
2) *Authentication:* involves building a strong two tier CAPTCHA solution that will help in detecting an illegitimate user from the legitimate as well as distinguish computer program from human users. For instance, when students or staff request for service through the cloud system, the system should be able to verify the identity and credential

before access to the institution’s network is granted

3) *Data encryption:* involves the process of transforming the data or information into undecipherable code before storage and during connection to other networks. It uses parameter or key to carry out the transformation and can be used to create a digital signature which allows authentication to be easily carried out on the user. It does not only help the learners or network providers but also helps to check insider attack of the cloud infrastructure. The higher institution alongside the cloud provider should determine which sensitive data to encrypt based on the organisational security policy. Traditional encryption algorithms such as Data Encryption Standard (DES), Triple DES algorithm (3DES), RSA (public key) algorithm, Symmetric Key Encryption, Advanced Encryption Standard (AES) and Blowfish algorithm techniques can be used to encrypt the different files on the system [12].

4) *Backup and recovery:* in backup and recovery, the cloud service provider could ensure regular data backup and this often involves sending a copy of the encrypted data to an offsite server hosted by another or third party service provider. However, the institutions could also do local backup or outsource this to other organisation. This will ensure an effective disaster recovery in case of a major attack on the cloud infrastructures.

5) *Authorisation and control:* authorisation and control are used to control accessibility to resources or services in cloud infrastructure. It is used to determine if the user has the privilege and right to access and perform a given action within the resources. This will include ensuring role-based access control, this simply means using the pre-determined position or roles of the user to determine authorisation to a certain level of information. For example, the management, staff and students authorisation level for access to data or information on the cloud infrastructure should be different and any privileges granted should be in accordance to the assigned role [18].

6) *Protection as a service:* involves providing protection mechanism for the cloud infrastructure that includes prevention of the occurrence of attacks and early detection of intrusion / attacks. The protection as a service will help not only the cloud platform but also the student-device level and network level protection.

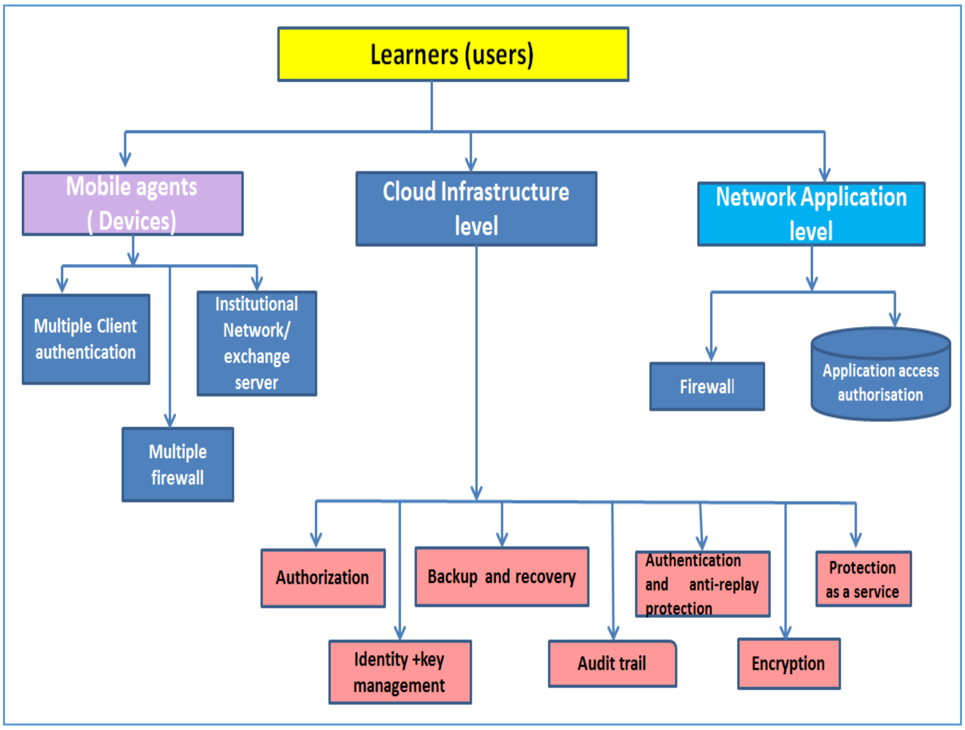
Learners (users)
Mobile agents (Devices)
Cloud Infrastructure level
Network Application level
Multiple Client authentication
Institutional Network/ exchange server
Multiple firewall
Firewall
Application access authorisation
Authorization
Backup and recovery
Authentication and anti-replay protection
Protection as a service
Identity +key management
Audit trail
Encryption

Fig.4. Proposed data protection and security architecture

VI. Conclusion and Future Research

M-learning technologies have significantly impacted the educational sector since its emergence and the benefits are innumerable. However, for it to be properly implement and fully adopted by different users in HEIs, the issues of security and data protection of m-learning deployed on cloud platform have to be adequately addressed.

This paper has examined the vulnerability issues relating to data protection and security of m-learning platform in cloud infrastructures. It also proposes multilayer platform architecture for the protection of learners and their data in cloud infrastructure. It is expected that from this framework, a sequential step will be developed for the implementation and validation of the framework in order to provide protection for the data and user of m-learning in cloud infrastructure. It is believed that most cloud platforms used for m-learning requires very strong security and data protection control. However, a trade-off must be made between the threat of the exposure of data and the efficiency of the architecture. This simply means the HEIs constantly need to reassess their IT security strategies as any breach of data security would result in grave financial implication, operational issues and loss of trust amongst others.

REFERENCES

[1] F. Bahry, N. Anwar, N. Amran, and R. Rias 2015. "Conceptualizing security measures on mobile learning for Malaysian higher education institutions". *Procedia-Social and Behavioral Sciences*, *176*, pp.1083-1088.

[2] D. Keegan, G. Dismihok, N. Mileva, and T. Rekkedal. (2006). "The role of mobile learning in European education". Work Package 4, 227828-CP-1-2006-1-IE-MINERVA-M, European Commission.

[3] A. Dias, J. Carvalho, D. Keegan, G. Kismihok, N. Mileva, J. Nix, and T. Rekkedal, 2008. "An Introduction to mobile learning". Work package.

[4] A. T. Korucu, and A. Alkan,, 2011. "Differences between m-learning (mobile learning) and e-learning, basic terminology and usage of m-learning in education". *Procedia-Social and Behavioral Sciences*, *15*, pp.1925-1930.

[5] A. Al-Hunaiyyan,, R. Alhajri and S. Al-Sharhan , 2016. "Perceptions and challenges of mobile learning in Kuwait". Journal of King Saud University-Computer and Information Sciences

[6] S. Oyelere, D. Sajoh, Y. Malgwi and L. Oyelere, 2015, November. "Cybersecurity issues on web-based systems in Nigeria: M-learning case study". In Cyberspace (CYBER-Abuja), 2015 International Conference on (pp. 259-264). IEEE.

[7] R. Buyya, C. Yeo, S. Venugopal, J. Broberg, and I. Brandic, 2009. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility". Future Generation computer systems, 25(6), pp.599-616.

[8] C. Low, Y. Chen, and M. Wu, 2011. "Understanding the determinants of cloud computing adoption". *Industrial management & data systems*, 111 (7), pp.1006-1023

[9] T. Ercan, (2010). "Effective use of cloud in educational institutions". *Science Direct. Procedia Social and Behavioural Science.* pp. 938-942. Elsevier

[10] P. Mell, and T. Grance, 2011. The NIST definition of cloud computing.

[11] C. Allison, A. Miller, I. Oliver, R. Michaelson. and T. Tiropanis (2012). "The Web in education". *Computer Networks*, 56 (18), pp. 3811-3824.

[12] R. Arora, A. Parashar and C. C. Transforming, 2013. "Secure user data in cloud computing using encryption algorithms". International journal of engineering research and applications, 3(4), pp.1922-1926.

[13] D.Morrill, (2011) "Cloud Computing in Education" Available at https://www.cloudave.com/14857/cloud-computing-in-education/

[14] A. Jain and U.S. Pandey, (2013). "Role of Cloud computing in higher education. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(7).

[15] R. Katz, P. Goldstein, R. Yanosky, and B. Rushlo. "Cloud computing in higher education." In EDUCAUSE.[Online],[Retrieved October 5, 2017], http://net. educause. edu/section_params/conf/CCW, vol. 10. 2010.

[16] S. Tout, W. Sverdlik, and G. Lawver (2009). *Cloud computing and its security in higher education.* [Online] Available from: https://www.researchgate.net/profile/Samir_Tout/publication/255618308_Cloud_Computing_and_its_Security_in_Higher_Education/links/553841300cf226723ab62be6.pdf [Accessed 15 March 2017].

[17] A. Singh, D. Shrivastava. (2012) "Overview of attacks on cloud computing". International Journal of Engineering and Innovative Technology (IJEIT). 2012 Apr;1(4).

[18] J. M. Calero, N. Edwards, J. Kirschnick, L.Wilcock, and M. Wray, 2010. "Toward a multi-tenancy authorization system for cloud services". IEEE Security & Privacy, 8(6), pp.48-55.

[19] I. Ivanov, (2011). "Cloud computing in education: the Intersection of challenges and opportunities". In: *International Conference on Web Information Systems and Technologies*, pp. 3-16, Springer, Berlin, Heidelberg.

[20] G. Feuerlicht, V. Snasel, P. Szczepaniak, A. Abraham and J. Kacprzyk (2010). "Next Generation SOA: Can SOA Survive Cloud Computing?" In: *Advances in Intelligent Web Mastering - 2* Springer Berlin / Heidelberg, pp. 19-29.

[21] R. N. Katz, P. Goldstein, and R. Yanosky, 2009. "Demystifying cloud computing for higher education". EDUCAUSE Center for Applied Research Bulletin, 19, pp.1-13.

[22] P. Pocatilu, F. Alecu, and M.Vetrici, 2010. "Measuring the efficiency of cloud computing for e-learning systems". *Wseas transactions on computers*, *9*(1), pp.42-51

[23] J. Staten, (2009). *Is Cloud Computing Ready For The Enterprise?* [Online] Available from: http://ceria.dauphine.fr/cours98/CoursBD/doc/Forrester-Cloud-computing-report080307%5B1%5D.pdf [Accessed 13 October 2017].

[24] L.M Vaquero, M. Rodero-Merino, J. Caceres and M. Lindner. (2009). Break in the Clouds: Towards a Cloud definition. *ACM SIGCOMM Computer Review*, 39 (1), pp. 50-55.

[25] L. Wang, J. Tao and M. Kunze (2008). "Scientific Cloud Computing: Early Definition and Experience". In*: the 10th IEEE International Conference on High Performance Computing and Communications*, 8, pp. 825-830. IEEE.

[26] A. Weiss. (2007). "Computing in the clouds". *networker*, *11*(4), pp.16-25.

[27] X. Li, Y. Li, T. Liu, J. Qiu, and F. Wang, (2009). "The Method and Tool of Cost Analysis for Cloud Computing". *2009 IEEE International Conference on Cloud Computing.* DOI 10.1109/CLOUD.2009.84, IEEE Computer Society.

[28] H. Suo, Z. Liu, J. Wan, and Zhou, K. (2013). "Security and privacy in mobile cloud computing". In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International (pp. 655-659). IEEE.

Authors' Profiles

Olugbenga W. Adejo holds a PhD in Computing Science from University of the West of Scotland in Paisley United Kingdom. Previously he received B.Sc. in Agricultural Economics at the University of Calabar, Nigeria, Advanced/Higher Diploma in Computer Science North Glasgow College as well as MSc in Information Technology (Application Development) from University of Sunderland, United Kingdom. His research focuses on Data Mining application, Big data analytic, learning analytic, Predictive analytics, Human Computer Interaction, and Business Modelling. He has written interdisciplinary papers on application of Information technology to agriculture, e-health and commerce as well as Learning Analytic in Education.

He is a member of the Association of Computer Machinery (ACM) and he currently serves as member of program and review committee of various International conferences around the world.

Isaiah Ewuzie obtained his B.Sc Geology in 2001, M.Sc IT (with Project Management) and a PhD in area of Cloud Computing. He has co-authored and presented several papers at international conferences. His main research interests include but not limited to cloud computing, IoT, e-learning, cyber security, data analytics and big data.

Abel Usoro (PhD) lectures in School of Engineering and Computing of the University of the West of Scotland. His research is in information systems which include knowledge management, smart cities, e-learning, m-government, e-hospitality and cloud computing. He has published widely in refereed journals and conferences. He has been a member of scientific committees of many international conferences which of which he has chaired.

He serves in the editorial committee of many refereed journals and is also the editor-in-chief of the Computing and Information Systems Journal. Over the years, he has been involved in business and information systems consultancies and projects in Europe (mostly UK and an EU project that involved other European countries), Africa (Nigeria) and the Pacific (Solomon Islands). He established strong Erasmus relationship between his institution and Laurea and Turku Universities of Applied Technology in Finland where he constantly visits.

Thomas Connolly is a Professor in the School of Engineering and Computing and the director of the Institute for Creative Technologies and Applied Computing, University of the West of Scotland. His current research activities include Serious Games, Computer Games, Digital Health, eLearning, Database Management Systems, SME Innovation, creativity and entrepreneurship. He was the designer of RAPPORT, the world's first commercial portable DBMS and the LIFESPAN configuration management tool.

How to cite this paper: Olugbenga W. Adejo, Isaiah Ewuzie, Abel Usoro, Thomas Connolly, "E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure", International Journal of Information Technology and Computer Science(IJITCS), Vol.10, No.4, pp.1-9, 2018. DOI: 10.5815/ijitcs.2018.04.01