About this paper

Appears in:
EDULEARN15 Proceedings
(browse)

Pages: 3857-3863
Publication year: 2015
ISBN: 978-84-606-8243-1
ISSN: 2340-1117

Conference name: 7th International Conference on Education and New Learning Technologies
Dates: 6-8 July, 2015
Location: Barcelona, Spain

Citation download:
(BibTeX) (ris) (plaintext)

Other publications by the authors:
(search)

CLOUD SECURITY AND THE INTERNET OF THINGS: IMPACT ON THE VIRTUAL LEARNING ENVIRONMENT

A. Atayero, S. Ilori, M.O. Adedokun

Covenant University (NIGERIA)

All Virtual Learning Environments (VLE) rely heavily on the cloud and its associated technologies.

The emerging Internet of Things paradigm will inevitability affect all spheres of human endeavors, the learning environment inclusive. A major concern of both proponents and detractors of the IoTs is that of cloud security. This is so since the integrity of any virtual pedagogical process is a function of the security of the cloud service provider. It is a commonly accepted fact that the success of any learning process is measured during the assessment stage, during which the integrity of examination materials remain sacrosanct. It follows therefore logically that anything/person/process that can breach the cloud security has successfully rendered the whole pedagogical experience futile. This is so since the singular most important objective measure of success in the learning process would have been compromised. It is revealed in literature that around 90% of the over 50 petabytes of information currently available on the Internet are as inputted either directly by humans or through pseudoautomatic modes using HumanComputer Interfaces. This is however about to change drastically in a world characterised by the internetworking of things (Internet of Things). A very obvious consequence of this ubiquity of interconnectivity is the inevitable deluge of massive data that will become available for private, public, shared, and/or monetized consumption. We are concerned in this study with the part of this data related to all areas of VLE. In this paper, we present a survey of generic cloud security issues visavis the VLE identified currently in the literature, and suggested methods of mitigating them.

We go further by extrapolating the prevalent scenarios and suggesting ways of mitigating the challenges of the escalated scenarios.

keywords: vle, cloud computing, internet of things (iot).