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

Aderemi A. Atayero, Olusegun A. Ilori, Michael O. Adedokun

Covenant University (NIGERIA)

Abstract

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 endeavor, 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 profile 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 remains 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 pseudo automatic modes using Human Computer Interfaces. This is however about to change drastically in a world characterized by the internetworking of things (Internet of Things). A very obvious consequence of this ubiquity of interconnectivity is the inevitable deluge of 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 *vis-à-vis* the VLE identified currently in the literature, and suggest 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.

1 INTRODUCTION

The anticipated increase in the number of things interconnected with one another (either over the Internet of via ad-hoc networks) will inevitably lead to an explosion of available data and information that will need to be processed and stored in the cloud. Wireless Sensor Networks (WSN) and intelligent embedded devices will not have the capacity to store the copious amounts of data that they will generate, or perform necessary data analytics on them. These services will have to reside primarily in the cloud [1]. The Virtual Learning Environment (VLE) is by definition a software solution that facilitates computerized learning using remote connectivity. It is an e-learning Education platform based on the web that provides virtual access to lectures, lecture content, tests, grades and assessments. It is also a social space where students and teachers can interact through threaded discussions or chat. It utilizes Web design tools and a content management system [2].

The Virtual Learning Environment (VLE) by virtue of its mode of operation depends on cloud facilities and services for various functions e.g. storage of learners' details, using the SAAS (Software as a Service) and IAAS (Infrastructure as a Service) functions of the cloud, *et cetera* [3]. The security and integrity of VLE data must remain sacrosanct for it to reliably achieve its e-learning objectives. It is therefore logical to expect that any (and every) thing that affects the integrity of cloud services will inevitably affect the sanctity of the VLE, especially as it concerns the assessment of learners' accomplishments of the learning objectives. A good proportion of the VLE data are of a personal or sensitive nature, therefore unauthorized access to them is not desirable. Compromising online storage, analytics or cognition services will necessarily lead to a corruption of the main objectives of virtual learning.

It is envisaged that the VLE cannot escape the pervasive onslaught of innovations and inventions that has become characteristic of the emerging sphere of the Internet of Things (IoT). A number of *Smart* gadgets and devices are already in existence for transforming the VLE into a *SmartVLE*. Such devices as already exist (and those that will be invented in the future) will have embedded in them WSN nodes and chips for various purposes, ranging from Learners' identity authentication (or verification) to geo-

tagging of devices used for virtual learning purposes. In this paper we draw attention to the importance of security in a cloud powered Internet of Things as it relates to the Virtual Learning Environment. We point out the undesirable effects that compromised cloud services can have on learners, e-learning institutions (or businesses) and Governmental agencies concerned with the VLE. Subsequently, we propose solutions to some of these security threats.

The rest of the paper is organized as follows: Section 2 gives the conceptual introduction of the cloud, the cloud security and its importance in the emerging IoT paradigm as it concerns the VLE. In Section 3, we consider the major security concerns of a cloud-based IoT system, especially in connection with the reliability of VLE-enabled cloud services. Solutions to identified sources of threat are proposed in Section 4, while the paper is concluded in Section 5.

2 THE CLOUD AND THE INTERNET OF THINGS

Recent developments as noted in the literature indicate that the new paradigm of the Internet of Things tilts towards a cloud powered Internet of things. Things will have limited processing, energy, communication bandwidth and storage. The marriage of the cloud and Internet of Things -"*cloudIoT*" paradigm, are discussed in [4]. In [5], an open application layer that aids interoperability of IoT devices is proposed. In this work, application logic is moved to the cloud -allowing device performance and behavior to be continuously monitored, fine-tuned and reprogrammed by the manufacturer or end-user. Full World Wide Web integration of embedded devices that might not have the resources to do have such an interface and cross-compatible APIs are a few of the motivations of this cloud powered IoT approach.

2.1 The Import Of Cloud Security To The Internet Of Things

The sheer scale, magnitude and value of data that the Internet of Things will process and store in the cloud, coupled with the fact that the data is located in one place will make these data more prone to attacks. Here, we examine the vulnerability of stakeholders (individuals, business and governments) to security issues in the cloud of things.

2.1.1 Threats To Learners

Virtual learners engage various platforms in the learning process. Vendors of mobile phones, smart devices and wearable computers store personal information such as health records, financial records, location; all collected in real time and pushed to the cloud. Unauthorized access to this sensitive kind of information maybe used by nefarious parties to spy on and corrupt the VLE. With the advent of the cloud of things, where cloud residing applications and services are used to manage and monitor the VLE, a compromised cloud service could potentially pose serious threats to the sanctity of the whole virtual learning experience.

2.1.2 Threats to VLE Businesses

Attacks against business owned cloud services will hurt the bottom line, leading to mistrust, loss of goodwill and credibility to businesses. This will equally affect the overall subscription rate to any particular VLE platform. An example is the *iCloud* breach of August 2014. Amazon's *EC2* and Google's cloud services have also had their fair share of challenges. A Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack, preventing IoT devices from reaching their cloud server will be quite harmful to a maker of such devices; as the devices will either not function at all or function with limited capability – an equally fortunate outcome for the attacker [1]. Later in this paper, we propose redundancy as a means for lessening the effects of these kinds of threats. The "*Cloud of Things*" will further escalate security problems currently encountered in the present cloud (mostly storing data belonging to people, not things) if security concerns are not promptly addressed.

2.1.3 Dangers To VLE Governmental Agencies

Cloud powered IoT infrastructure will be of great help to governmental agencies, seeing as WSN will provide real-time data and backend cloud services can perform analytics on data fetched. Agencies can become more effective and responsive to the needs of people. However, attacks to cloud powered or enhanced critical IoT infrastructure (energy, transportation, public health and emergency services) can have grave consequences for governmental agencies in general [6]. Attacks on government owned cloud infrastructure are usually insidious in nature. For example, malware that

slightly corrupts the results of cloud hosted analytics (or VLE assessment results). The results of such processing may then be used to form "informed" policies that will favor the attacker (or group of concerned learners). Though such attacks will be sophisticated and somewhat difficult to implement (and track), these kinds of compromise can have far reaching implications on the credibility of VLEs. Indeed, if the security concerns of cloud computing are not properly and promptly addressed, it may slow down the adoption of cloud powered IoT devices and subsequently their application in various domains, including VLE. Presently, IT professionals have slowed down the adoption of cloud services due to security concerns [7]. Compromising timely access to information or cloud processes may lead to incorrect operation of actuator. Ultimately, one of the gravest concerns in a world powered by cloud-enabled things is that they will have access to, and the capacity for manipulating not just information, but physical objects –the physical world.

3 SECURITY CONCERNS OF A CLOUD-POWERED INTERNET OF THINGS

In this section, we examine security concerns of cloud computing as identified in current literature and point out what these security issues might portend in a cloud-powered IoT as it relates to the VLE. In our analysis of the current security risks facing the cloud, we shy away from strict segregation of cloud services and models. For example, we neither delineate Platform as a service (PAAS), Software as a service (SAAS), and Infrastructure as a service (IAAS) nor do we demarcate between public, private and hybrid clouds. The lines that separate these services and models are getting increasingly blurry. It is clearly understood that security issues in lower layers are inherited by the layers above them (e.g. PAAS inheriting security risks from IAAS, and SAAS inheriting from PAAS and IAAS). Many of the security concerns in cloud computing are quite clearly understood and clearly elaborated in the literature [8]. Usually, they revolve around the themes of, data security, network security, availability, authentication and legal concerns [10]. Another argument goes that parallels can be drawn between cloud computing and previous time-sharing computer systems that the issues truly unique to cloud computing are the complexities of multi-party trust considerations and the need for mutual auditability [9]. In the analysis that proceeds, we thematically group the cloud security issues, and examine the risks that these security issues portend to the IoT.

3.1 Access Control

This refers to *who* has access to *what* and to *what degree*. Access control entails physical access to cloud servers as well as authentication and authorization of users. Access control – identity and access management is the first line of defense – privacy and data security in the cloud would not be possible without levels of privilege. As relates to the Virtual Learning Environment, access control is a major determinant of the success of the whole pedagogical experience. If imposters are able to access the learners' platform, then assessment becomes compromised and degree of success in accomplishing the learning objectives cannot be ascertained.

3.2 Data security

A major security concern of consumers of cloud services (including the VLE) as well as cloud providers who must guarantee a minimum level of security to clients is the security of data at rest and in transit. Encryption of stored and transmitted data is the usual solution. Regarding data segregation resulting from shared computational resources, encryption may still be the most viable solution to securing data at rest. Cloud servers have been demonstrably employed in gleaning data from co-resident virtual machines (e.g. on Amazon's EC2 servers). *VLE-enabled* IoT devices will mostly push and request small amounts of data from cloud servers, makers of such devices will need to consider how confidentiality of end users may be compromised by monitoring patterns of data in transit and how proprietary software may be reverse engineered by observing network traffic. When data is deleted or infrastructure is decommissioned, how data is ultimately disposed of must be clearly known. A lot of information can still be gotten from the small chunks of data that "*things*" forward to the cloud.

3.3 Reliability and Redundancy of *VLE-Enabled* Cloud Services

The reliability and availability of cloud services is of paramount importance in the IoT. *VLE-enabled* IoT devices with limited storage and computational capabilities, once shipped must have their cloud resources online to function fully if at all. By their very nature, these cloud-connected things will have little or no direct human supervision. In this wise, long-term viability of cloud service provider, backup of data, redundant resources and availability of cloud resources are critical. For things that rely on the

result of analytics performed on reams of data generated at various sources, the loss of such data can be catastrophic.

3.4 Legal Issues

The geographical location of data stored in the cloud – data locality; privacy and data protection laws in particular areas; international laws; and laws governing electronic devices usage and wireless communication all sit together in the melting pot of a cloud powered IoT. The legal implications of production and usage of the plethora of "things", either cloud-connected or stand-alone, are yet to be fully understood by all stakeholders. The input of accreditation bodies of individual nations also becomes necessary. For example, it is a commonly accepted notion that the engineering discipline is not quite suited for the VLE. The argument in support of this notion is usually that in the instruction of engineering courses, hands-on laboratory exercises cannot be dispensed with.

3.5 Standard Practices and Regulatory Compliance

The willingness and ability of a cloud service provider to comply with standard industry practices and regulations, as well as willingness to submit to being externally audited communicates the level of reliance clients can hope to put on such a provider. Compliance with industry standards must be put into due consideration. For example, devices and applications that need to store personal health records will need to be HIPAA-Compliant. Mutual auditability extends the idea of auditing a little further and by this we mean that clients are going to need to also submit to being audited.

4 SOLUTIONS TO THREATS IN THE CLOUD-OF-THINGS

In this section, we propose solutions to some of the security issues examined in section 3. Some of the solutions proposed can be readily implemented using current technologies, while others will take a few more years before they can be implemented.

4.1 Re-imagining The Service Level Agreement (SLA)

The Service level agreement (SLA) is the only legally binding document that the provider of a cloud service has with the consumer. It states the minimum level of service that a customer can hope to expect, necessary actions when such expectations are not met, how conflicts are redressed, and so forth. However, there is a plethora of legal *verbiages*, metrics, and cloud standards that ultimately lead to ambiguity, confusion and conflict [11]. The European Commission provides a guideline for standardizing the SLA [12]. The document addresses neutrality of technology, business model, vocabulary, etc. This guideline deals mainly with issues that have to do with cloud services delivered to people and not to things. A number of cloud security risks, many of which have been discussed in this paper, and how they can be addressed by SLA are examined in [13].

Addressing cloud security issues with an SLA becomes increasingly nebulous as it relates to VLE-enabled IoT. Ultimately, the quality of a cloud service is determined by the standard of service that the consumer gets. Taking into consideration network characteristics, the reliability of the embedded device itself and various other features, how will performance of cloud services be objectively measured? When does an SLA come into force with a "thing"? How do these contracts come up for review? What will be the procedure for terminating the contracts? These are some of the open questions yet to be addressed. IoT devices are designed to operate with minimal human intervention; as such current SLA practices may need to be reviewed with the cloud powered IoT.

4.2 Fully Homomorphic Encryption

Homomorphic encryption has a powerful potential for protecting data in the cloud of things. In one fell swoop, it provides a viable solution to three important security concerns in the cloud: a) *data security*, b) *third party control* and c) *privacy issues*. Homomorphic encryption allows data to be processed in the cloud without a need for first decrypting it. IoT devices can safely leverage on the enormous computing power available in the cloud. Cloud computers processing data in encrypted form can make statistical deductions, learn patterns and predict trends by virtue of the large data sets that they receive from several IoT devices. Encryption is a known method for solving the problem of data remanence - the residual representation of digital data that remains even after attempts have been made to remove or erase the data [14]. Since cloud-computing platforms are available on a rental (as service) basis, whatever residual data is left in the cloud remains encrypted.

Here, we examine the fully homomorphic encryption scheme proposed in [15]. It allows any party, to carry out functions $f(\pi 1, \ldots, \pi t)$ on $\pi 1, \ldots, \pi t$, without revealing any information about the functions carried out or decrypting the plain text. The plain text, πi, is encrypted using a public key (pk) known to all parties. The encryption produces a ciphertext ψi as shown in (1). Encryption is done before the data is forwarded to the cloud.

$$\psi \mathrm{i} \leftarrow \mathrm{Encrypt}\, \varepsilon(\mathrm{pk}, \pi \mathrm{i}) \tag{1}$$

Computations can be carried out on the ciphertext ψi using any circuit C – a circuit can query the ciphertext, write to it, perform mathematical or statistical operations, anything that can be efficiently described as a circuit – and return the result, also a ciphertext. Evaluate function shown in (2) carries out the relation described above. In the cloud, functions are carried out on the ciphertext

$$\psi \leftarrow \mathrm{Evaluate}\, \varepsilon\, (\mathrm{pk}, \mathrm{C}, \psi 1, \ldots, \psi \mathrm{t}) \tag{2}$$

Upon successful computation in the cloud, the result – a ciphertext, ψ, is forwarded to the IoT device, which proceeds to decrypt it using a key known only to itself and safely implement the results.

$$\mathrm{Decrypt}\, \varepsilon(\mathrm{sk}, \psi) = \mathrm{C}(\pi 1, \ldots, \pi \mathrm{t}) \tag{3}$$

A further description of a method for circuit privacy is given in [3], thus further increasing the security of a fully homomorphic encryption scheme. Gentry's fully homomorphic encryption scheme requires a fair amount of computational resource. However, it is a reliable way to securely process sensitive data in the cloud.

4.3 Building Redundancy Into Cloud Services and Things

4.3.1 Quantum Computing - The Potentials for Cloud of Things

Quantum computers will be able to process certain kinds of information exponentially faster than current digital computers. D-Wave so far has been able to efficiently solve optimization type problems. This will prove to be very useful with WSN churning out a lot of data that must be promptly analyzed and processed. The D-Wave has been used to find bugs, anomaly detection in computer code, -a feat currently impossible on digital computers. Anomaly detection using computation [16], will shows great promise, it may help cloud servers detect any kind of irregularity resulting chiefly from unauthorized data access, or processing –resulting from an attack. The cloud of things will be largely unsupervised by direct human intervention; and result of computations done in the cloud will, in many cases, used to actuate mechanical systems; inconsistencies in cloud server output can be immediately checked in the cloud by quantum computation before being forwarded to the device that consumes such data.

4.3.2 Mutual Auditability

Cloud services providers in the future must be more accountable to users about what their data is used for; what kinds of analytics are performed on them, etc. In a world where IoT devices can manipulate the real world, mutual auditability can help clarify establish culpability. The main motivations for this kind of Logs can also be useful to forensic investigators in case of incident [17].

4.3.3 Legislation of "Cloud of Things"

The paper above refers to the case of data protection legislation in Germany and Sweden. The location of data holding servers and the laws of the land to these data. Legislation must be drawn up to establish who is culpable in the situation of an attack such as who will be liable in case of accidents.

4.3.4 Securing The VLE-Enabled Cloud of Things

In this case study, we will illustrate how the security concerns of an IoT powered VLE system are mitigated using some of the methods discussed above. Learners' Personal Record (LPR) is very sensitive in nature for VLEs. Here we propose how LPR can be secured in the cloud. The proposed method is based on the idea that all records, academic history, current courses, geo-tagging sensor reading, course materials, assignments etc. made by cloud cognitive services (e.g. *IBM Watson*) are all stored in the cloud. A learner-centric scalable, secure LPR system akin to one discussed in [18] is then used to retrieve LPR from the cloud on a need to know basis. The patient himself controls access to his/her LPR by various stakeholders: Academic Adviser, Dean, Head of Department, etc. In the cloud, homomorphic encryption techniques [3] are used to allow processing and yet limit visibility to

LPR data. This method can provide anonymity to individuals, while improving the quality of service delivery.

5 CONCLUSION

In this paper we have examined some of the security concerns that a cloud-powered Internet of Things (IoT) will present as it relates to the Virtual Learning Environment. We suggest ways that the large volume of data web-connected things will provide can be secured in the cloud, how analytics can be safely performed on large datasets using homomorphic encryption and cloud computing. While it is true that a cloud powered IoT has numerous and profound advantages, security is a big concern. As noted by Kevin Ashton – the man who first coined the phrase "*Internet of Things*" in [19]: "*The Internet of Things has the potential to change the world, just like the Internet did. Maybe even more so*". But for the IoT to fully take off, the security issues discussed in this paper, and particularly those that have to do with VLE must be thoroughly examined and mitigated by all stakeholders.

REFERENCES

[1] Atayero A., Oshin O., Oshin B., Alatishe A. (2014s), "Distributed Denial of Service (DDoS) Network Attacks: Impact On The Virtual Learning Environment", Proceedings of 7th ICERI, pp. 2235-2240, ISBN: 978-84-617-2484-0, Nov. 17th-19th, 2014 Seville Spain.

[2] Atayero A., Alatishe A., Oshin O., (2014r), "30 Billion Devices Automatically Interconnected By 2020: Impact On The Virtual Learning Environment", Proceedings of 7th ICERI, pp. 2326-2331, ISBN: 978-84-617-2484-0, Nov. 17th-19th, 2014 Seville Spain.

[3] Atayero A.A, Feyisetan O. "Security issues in cloud computing: The potentials of homomorphic encryption." Journal of Emerging Trends in Computing and Information Sciences 2, no. 10 (2011): 546-552.

[4] Botta A., De Donato W. Persico V., and Pescapè A. "On the Integration of Cloud Computing and Internet of Things", Proceedings of the 2nd International Conference on Future Internet of Things and Cloud (FiCloud-2014). 27-29 August 2014, Barcelona, Spain

[5] Kovatsch, Matthias, Simon Mayer, and Benedikt Ostermaier. "Moving application logic from the firmware to the cloud: Towards the thin server architecture for the internet of things." Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on. IEEE, 2012.

[6] http://csrc.nist.gov/groups/SMA/fisma/documents/rmf-sz.pdf accessed Sept 2014

[7] Ponemon Institute, "Security of Cloud Computing Users Study", accessed May 2015, available: http://bit.ly/1HzIjzp, Mar. 2013.

[8] Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of Network and Computer Applications 34.1 (2011): 1-11.

[9] Chen, Yanpei, Vern Paxson, and Randy H. Katz. "What's new about cloud computing security." University of California, Berkeley Report No. UCB/EECS-2010-5 January 20.2010 (2010): 2010-5.

[10] Brodkin, Jon. "Gartner: Seven cloud-computing security risks." Infoworld 2008 (2008): 1-3.

[11] Gleeson, Niamh Christina, and Ian Walden. "'It'sa jungle out there'?: Cloud computing, standards and the law." European Journal of Law and Technology5.2 (2014).

[12] European Commission (2014). "Cloud Service Level Agreement Standardisation Guidelines." Brussels, Belgium.

[13] Balachandra K., Reddy V, Paturi R., and Rakshit A.. "Cloud security issues." Services Computing, 2009. SCC'09. IEEE International Conference on. IEEE, 2009.

[14] Data remanence, http://en.wikipedia.org/wiki/Data_remanence

[15] Gentry C., A fully Homomorphic Encryption Scheme Ph.D. thesis, Stanford Univ., Dept. of Comp. Science, 2009.

[16] Pudenz, K. L., & Lidar, D. A. (2013). Quantum adiabatic machine learning.Quantum information processing, 12(5), 2027-2070.

[17] http://www.cepis.org/media/CEPIS_Cloud_Computing_Security_v17.11.pdf

[18] Vidya, S., K. Vani, and D. Kavin Priya. "Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing." InInternational Journal of Engineering Research and Technology, vol. 1, no. 10 (December-2012). ESRSA Publications, 2012.

[19] Ashton K, “That Internet of Things Thing” Rfid Journal (Jun 2009).