Journal of Computer Networks, 2019, Vol. 6, No. 1, 1-7
Available online at http://pubs.sciepub.com/jcn/6/1/1
Published by Science and Education Publishing
DOI:10.12691/jcn-6-1-1

An Intelligent Client-Trusted and Dependable Security Framework to Ease Smartphone Portability on Community Cloud-Computing

Rume Elizabeth YORO[1], Arnold Adimabua OJUGO[2,*]

[1]Department of Computer Science, Delta State Polytechnic Ogwashi-Uku, Delta State, Nigeria
[2]Department of Maths/Computer Sci., Federal University of Petroleum Resources, Effurun
*Corresponding author: ojugo.arnold@fupre.edu.ng

Received September 15, 2019; Revised October 24, 2019; Accepted November 21, 2019

Abstract Cloud computing is a relatively new technology that is in wide use because of the benefits it offers but is still confronted with security issues. The residence of the client's sensitive or proprietary data in the cloud service provider's server and premises expose the data to the possibility of manipulation, modification, inspection, deletion or theft. This possibility creates fears in the mind of the data owner and reduces the user's trust level in cloud computing. We propose a client trusted security framework to increase users trust level in cloud computing to make it more dependable. The proposed framework includes a user focused software process model for cloud computing security. Formal analysis of the proposed framework shows that it is capable of increasing the trust level of cloud computing by about 67 % when implemented by cloud service providers.

Keywords: *cloud computing, users trust, framework, model*

Cite This Article: Rume Elizabeth YORO, and Arnold Adimabua OJUGO, "An Intelligent Client-Trusted and Dependable Security Framework to Ease Smartphone Portability on Community Cloud-Computing." *Journal of Computer Networks*, vol. 6, no. 1 (2019): 1-7. doi: 10.12691/jcn-6-1-1.

1. Introduction

Cloud computing is relatively new and has no long history. In general it originates from the late nineties and has been further developed in the next millennium; the name was created because the data sent could not be tracked anymore when moving towards its destination. The term cloud was created because you could not determine the path a certain data package followed.

Cloud computing is stated into different definitions. There are definitions that define a cloud as a somewhat updated version of utility [1]. The other, and broader, side states that anything you can access outside your firewall is cloud computing, including outsourcing [2]. We adopt the agreed definition of the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance and define cloud computing as a model for enabling convenient, on-demand network access to a 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 [3]. In general, cloud computing provides hardware and software services that are in the cloud and can be accessed by client as they pay for it. But despite the various benefits of cloud computing, such as economies of scale, reuse and standardization [4], many are not comfortable with it because of the various risks and challenges that it portends. Cloud computing services includes Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Component as a Service (CaaS) [5,6,7]. Examples of IaaS cloud computing applications are: a cloud web server, a cloud data-center, and a corporate virtual desktop. A cloud data-center is a network of virtual servers that allows a company to move all of its corporate data assets into the cloud.

While there is no universally accepted definition of dependable cloud computing, its components and meaning must be clarified. Dependable cloud computing can be viewed as cloud computing which everybody (mainly consumers or information owners) can rely on to do what they want or need with all the security concerns adequately taken care of and data integrity is not compromised. Security concerns of cloud computing has been one of the drawbacks affecting the full adoption of cloud computing by many organisations [8].

2. Background of Study

Data and application in the cloud reside in systems the user does not own and likely has limited control over [4], this is responsible for the security issues associated with cloud computing. Some of the security concerns of prospective cloud service users include: possible harm to their organization for public and wide distributed access, the cost of such harm and the risk associated with possible cloud service failure [8,9]. These issues generate questions in the mind of prospective cloud users and when these questions are left unanswered, they feel insecure in adopting cloud computing despite all the possible gains that cloud computing provides.

2.1. Adopting Cloud Computing

Cloud Computing is also about how Information Technology (IT) is provisioned and used and not only about technological improvements of data centers [10]. Enterprises must consider the benefits, drawbacks, usage practices and other effects of Cloud Computing before adopting and using it [11]. In enterprises, the adoption of Cloud Computing is much dependent on the maturity of organizational and cultural processes as the technology per see [12]. Some predict that adoption of Cloud Computing is not going to happen overnight, rather it could take 10 to 15 years before a typical enterprise makes this shift [13]. Hence, we are currently at the start of a transition period during which many decisions need to be made with respect to adoption of Cloud Computing in the enterprise. In adopting Cloud Computing, enterprises will typically consider organizational clouds based on heterogeneous computing environment managed by more than one public cloud provider. The adoption of Cloud Computing does not depend only on technical issues but also the on risk management policy of the organization and the consideration of trade-offs between the benefits and risks [8,14,15].

Many of the risks and security concerns of cloud computing can be safely handled by organizations through planned risk management business processes and activities. Examples of such risks that enterprise must properly manage include: the right choice of service provider, the legal responsibility that must be accepted by service provided, the threat of access to intellectual properties and the content of disaster recovery documentation [3].

2.2. Data Security in Cloud

Lack of control on the physical infrastructure is responsible for most of the security issues which arise in Cloud Computing. Furthermore, enterprises are ignorant of the physical location of their stored data in the distributed environment and the type security mechanisms put in place by the cloud provider [16]. Other technical security issues in Cloud Computing relate to the problems of web services and web browser and not of Cloud Computing. The common use of web browsers and web services to access the services offered by the cloud make this issues still current and relevant. to access the services offered by the cloud The common attacks on web services include the XML Signature Element Wrapping, where XML signature is used for authentication [17,18].

Security controls in Cloud Computing are similar security controls in any IT environment. However, Cloud Computing may present, different risks to an organization because of service models, operation models and technologies associated with it. In cloud computing security controls models can be applied to applications using firewalls, to information using database activity monitoring, to management using configuration management and monitoring, to network using firewalls and to computing/storage using encryption. Using traditional security controls such as access controls and encryption, monitoring of large internal data migrations with Database Activity Monitoring and File Activity Monitoring; and monitoring of data moving to the cloud with URL filters and Data Loss Prevention. Other levels of encryption, to protect data moving to and within the cloud, are client/application encryption, Link/Network encryption and proxy-based-encryption and IaaS storage encryption, PaaS and SaaS encryption [4,19].

2.3. Virtualization and Trusted Computing

Virtualization is the process of decoupling hardware from the operating system on a physical machine [20]. Cloud computing provides to users multiple isolated users environments knows as virtual machines (VMs) on a single host [21]. A Virtual Machine (VM) is the virtualized representation of a physical machine that is run and maintained on a host by a software virtual machine monitor or hypervisor. An example of a Type 1 hypervisor is Xen [22]. Xen provides full virtualization to partition the host machine into multiple VMs. Trusted computing is a mechanism that allows organizations to verify their security posture in the cloud through hardware and software controls. Its key component is the Trusted Platform Module (TPM), which is a cryptographic component that provides a root of trust for building a trusted computing base. The goal virtual TPM (replacing TPM) or any trusted component is to move cryptographic computations into a locked virtual area, which is not under control of entities on the host platform [23,24]. However, TPM works only in non-virtualized environments. Therefore, a Virtual Trusted Platform Module (VTPM) is usually provided according to standard specification by creating an instance of TPM for each VM on a trusted platform [25,26].

3. Related Works

Various study groups and researchers have proffered remedies to the perceived flaws that come with cloud computing and there are other ongoing research work on this same subject matter of making cloud computing dependable.

Krautheim [26] proposed a model named Private Virtual Infrastructure that shares the responsibility of security in cloud computing between the service provider and client together with “Locator Bot” which pre-measures situational awareness through continuous monitoring of the cloud security. Jrad et al. [27] proposed a broker-based framework for running workflows in a federated environment that involves multiple Clouds. The framework is based on workflow management for the cloud. Anisetti et al. [28] proposed a certification framework that implements a security certification process for the cloud. The framework is a test-based security certification framework, in contrast to cloud security certification assurance technique, to support cloud providers in the design and development services and applications ready to be certified. Alqahtani et al. [29] proposed a context-based security framework for cloud services using aspect orientation to separate between business logic and security code. The framework focused on front end web services security to the cloud service. Considering security concerns, privacy and other business and technical risks associated with migration into cloud, Islam et al. [30] proposed a decision framework model for migration into cloud. The framework is a process model that considers the requirements and the risk of migration without providing a solution to cloud security issue. Rongyu et al. [21] proposed a user-specific virtual Trusted Platform Module and a trust chain model for virtual machines.

Sharma et al. [31] proposed a framework for implementing trust in cloud computing by integrating trust at the Infrastructure as a Service (IaaS) level. The framework employs an algorithm based on fuzzy logic to find trust. Rahaman and Farhatullah [5] proposed a three layered framework for preserving cloud computing privacy with an algorithm to generate unique user cloud identity. The goal of this framework is to preserve sensitive information entered by cloud users as they interact with the cloud to gain access to cloud services. Trabelsi et al. [32] proposed a privacy and security framework for mobile and cloud platforms. The framework is a symmetric architecture to address the problem of isolation of security and privacy requirements in the two platforms [33,34,35]. Poh et al. [36] proposed an authentication framework for peer-to-peer cloud network, the objective of which is to provide solution to authentication challenges in peer-to-peer cloud network in contrast to centralized cloud model. Youssef and Alageel [37] proposed a framework for the identification of security and privacy challenges in cloud computing. The same work also proposed a generic model to satisfy security and privacy requirements in clouds to advise users and protect against vulnerabilities. As the main contribution, this work proposes a client trusted security framework for dependable cloud computing using an integrated client trusted software process model, an approach that is distinct from previous efforts and supported by [34,35,38]. Our proposed model defines the association and relationship between the provider, the client, the client trusted process model and cloud service models.

4. Research Methodology

Systems analysis and design methodology was used for this study. Various cloud security frameworks and methods were studied to identify their strengths and drawbacks though literature survey to propose a new framework to enhance the strength of existing frameworks and to overcome some of their weakness. A client trusted security framework is proposed to make cloud computing more dependable.

4.1. Proposed Client Trusted Security Framework

The proposed framework consists of four major interacting and associated units. These are: Provider, Client Trusted Model, Cloud Service Models and Client. The Provider represents the cloud service providers. Examples of Providers are: Amazon, Google, Salesforce, IBM, Microsoft and Sun Microsystems who possess established data centers for hosting Cloud computing applications. The Client represents the cloud users. The Client includes enterprise service consumers with global operations, and all the consumers that pay service providers based on their usage of these utility services. Cloud Service models include includes Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) consisting of virtual machines, physical machines, resource allocator, other infrastructures and datacenters which are maintained continually by service providers. The Client Trusted Process Model is shown in Figure 2. It consists of two levels: the Provider's level and the Client's level which are linked together with a feedback. The provider's level consists of five basic operations with their deliverables. The Client's level consists of two operations with client's feedback as its deliverable. Client Trusted Process Model is described in the next section [39,40].

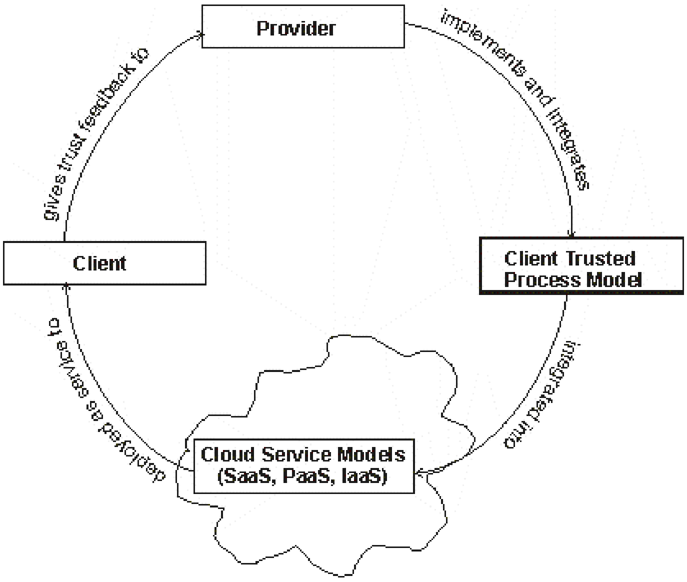
Provider
implements and integrates
Client Trusted Process Model
integrated into
Cloud Service Models (SaaS, PaaS, IaaS)
deployed as service to
Client
gives trust feedback to

Figure 1. The Conceptual Security Framework for Client Trusted Cloud

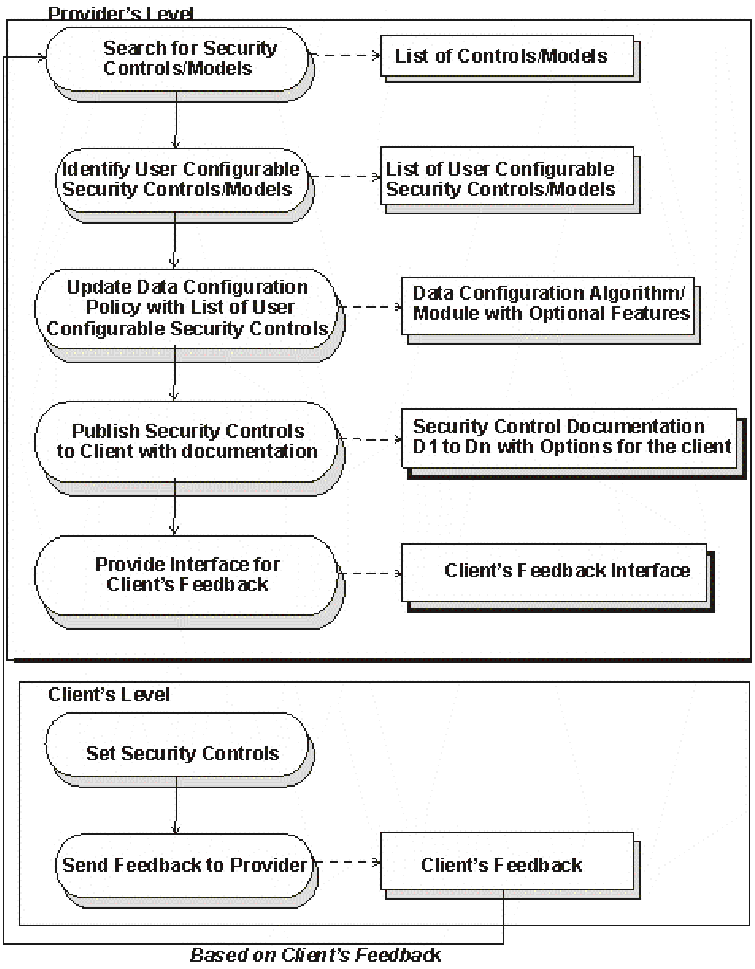
Provider's Level
Search for Security Controls/Models
List of Controls/Models
Identify User Configurable Security Controls/Models
List of User Configurable Security Controls/Models
Update Data Configuration Policy with List of User Configurable Security Controls
Data Configuration Algorithm/ Module with Optional Features
Publish Security Controls to Client with documentation
Security Control Documentation D1 to Dn with Options for the client
Provide Interface for Client's Feedback
Client's Feedback Interface
Client's Level
Set Security Controls
Send Feedback to Provider
Client's Feedback
Based on Client's Feedback

Figure 2. Client Trusted Process Model

Figure 1 shows the interaction and relationship among the four units of the framework. The provider implements and integrates Client Trusted Process Model. For IaaS, this integration of Client Trusted Process Model into the Cloud Service Models is done under the Data Configuration policies of IaaS data layer life cycle. The life cycle process of IaaS data layer includes the following phases: Data Configuration policies, provision of easy access to data, policy monitoring, calculation of Trust Factor Index and its implementation [23]. The Cloud Service Models are deployed to the Client 's as services. The Client gives his perception of trust to the Providers for Providers information and action.

4.2. Client Trusted Process Model

As seen in Figure 2, the client trusted process model consists of two levels: the Provider's level and the Client's level which are linked together with a feedback. The provider's level consists of four basic operations.

The first operation of Client Trusted Process Model at Provider's level is "Search for Security Controls/Models". This operation requires the domain knowledge of provider's software architect in cloud computing domain. Some of the available security controls and models have been discussed under background of study. The security controls must be classified into user-configurable and non-user configurable. The deliverable of this first phase and its exit criteria is the "List of Controls/Models". This list is the input into the next phase and operation.

The second operation is "Identify User Configurable Security Controls/Models". Security controls which the providers deliberately make available to the users for the purpose of building the users confidence are here referred to user configurable security controls. For example, a user may be allowed to configure two fac tor authentications but may not be allowed to gain access database activity monitoring. The deliverable of this phase is the "List of User Configurable Security Controls/Models".

The third operation is "Update Data Configuration Policy with List of User Configurable Security Controls". This phase involves writing the data policy configuration algorithm and providing the configuration module with optional security features for the client's use. The exit criteria of here, is data configuration algorithm and the operational module.

The fourth operation of the Client Trusted Process Model is "Publish Security Controls to Client with documentation". In this phase, the client is exposed to the various security features that he can apply to prevent the client's data from illegal access, theft, unauthorized migration etc. in the cloud. The exit criteria here, is the provision of labeled documentation D1 to Dn. A documentation Dn is attached to each security control feature exposed the client. Each major security control feature will increase th e level of trust of the user by a unit factor.

The fifth and the last operation of Client Trusted Process Model at Provider's level is "Provide Interface for Client's Feedback". In this phase the user is presented with the opportunity to send a feedback to the Provider on his level of trust and confidence.

The Client's level of Client Trusted Process Model captures the user's security responsibilities. The Client's level consists of two operations with client's feedback as its deliverable. The two operations are "Set Security Controls" and "Send Feedback to Provider". The user sets security control options and based on his experience and assessment of level of trust, the user sends a feedback to the Provider. The content of the user's feedback determines the next operation at the Provider's level. The operations of the process model terminate at a high level of user 's trust rating.

5. Framework Implementation Instance and Analysis

The proposed framework was tested through comparison and evaluation with a live and currently running scenario of a cloud provider and a user. The user subscribed for IaaS to a US based cloud service provider for the purpose of installing some proprietary applications. The product details as provided by the cloud provider, the options available and the values set are shown in Table 1. The fourth phase of Provider's level of Client Trusted Process Model of the proposed framework requires documentation. The documentation provided in the live and running cloud scenario is shown in Table 2.

Table 1. Cloud Provider's Product Options for the Existing Cloud System

Product Details	Options set
Registration Date:	5/27/2012
Product/Service:	Online Traders - Trader's VPS Value Edition
CNS Subscription ID:	118223
VM:	VM118223.tradersvps.net
IPv4 Address:	173.228.134.65
Number of Snapshots:	1
CPU Cores:	2
RAM (MB):	640
DISK (GB):	20
Two-factor Authentication:	No
VNC:	Do not install VNC
OS:	Traders VPS Windows 2003 (x86) Enterprise Edition R2
Language:	English
Datacenter:	NYC
Payment Method:	MasterCard, Visa & American Express
First Payment Amount:	$30.00 USD
Recurring Amount:	$30.00 USD
Next Due Date:	8/27/2016
Billing Cycle:	Monthly
Status:	Active

The location of the datacenter, the description of the Virtual Machine, the monthly rate paid by the user, the security control provided by the provider and other product information are shown in Table 1. It can be seen from Table 1 that the only security control provided by the provider is "Two-factor Authentication".

Table 2 Security Control with Documentation for the Existing Cloud System

Security Control Name	Documentation Label	Documentation
Two-factor Authentication	D1	Anytime you login from a device that you haven't verified in the last 12 hours, you will be asked to enter a token from the Google Authenticator app on your mobile device. You will be propmted to reverify again after 12 hours or after you actively log out by clicking "Logout" in the control pane. You can also request a token be sent to you via SMS if you do not have a smartphone that supports Google Authenticator. Simply enter the token displayed and your device will be verified for 12 hours, or until you log out.

The security control with documentation for the proposed framework using simulation is shown in Table 3. The instance of the proposed framework uses three security control systems:

Table 3. Security Control with Documentation for the Existing Cloud System

Security Control Name	Documentation Label	Documentation
Two-factor Authentication	D1	Anytime you login from a device that you haven't verified in the last 12 hours, you will be asked to enter a token from the Google Authenticator app on your mobile device. You will be propmted to reverify again after 12 hours or after you actively log out by clicking "Logout" in the control pane. You can also request a token be sent to you via SMS if you do not have a smartphone that supports Google Authenticator. Simply enter the token displayed and your device will be verified for 12 hours, or until you log out.
Use secure provisioning and Secure Migration Protocols	D2	These protocols prevent information from ever being sent to malicious hypervisor, virtual machines and host whenever a new virtual server is requested in the cloud. It puts a verification mechanism in place to ensure that that attacks against the virtual environment of your stored application or data will not be performed by an unapproved Operating System.
Virtual Trusted Platform Module	D3	Virtual TPM protects its internal data from being accessed by the host environment, hypervisor, and all other virtual environments on the platform and puts a protection in place to prevent itself from being cloned and it is maintained in a secure location under your full physical control

The user trust level increases with the number of operational and well document security controls. Comparing Table 2 with Table 3, the proposed framework is capable of increasing the trust level of the client by about 67 % when compared to the existing cloud system. The users trust can increase above this value as more appropriate security controls are put in place to clear the user ’s doubt and enhance the trust level.

6. Conclusion and Future Work

This work represents a new paradigm of information protection and security in cloud computing using a client trusted process model. We examined and defined a new client trusted security framework cloud computing. The proposed framework defines association and relationship between the cloud provider, the client, the client trusted process model and cloud service models. Formal analysis shows that the proposed framework is capable of increasing the user ’s trust level by about 67%. Cloud computing will gain a wider global acceptance if a client trusted security framework is employed and the user is made to participate in the configuration of well documented security controls accompanied with the provision of feedback to the cloud provider until absolute confidence of the user is gained. Future work shall focus on full scale implementation of this framework and how to protect the cloud from intentional malicious acts by the cloud provider.

References

[1] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems 25 (2009) 599_616, Elsevier.

[2] Knorr, E. (2008). What cloud computing really means. Available at: http://www.infoworld.com.d.cloud-computing/what-cloud-computing- really-means-031.

[3] ISACA White Paper. (2009). Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, IL, USA, pp 1-10.

[4] Van-Antwerp, A. L., Scoboria, K., Santos, J. R. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance. In: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf. Accessed: 15th July 2-16.

[5] Rahaman, S. M., Farhatullah, M. (2012). A framework for preserving privacy in cloud computing with user service dependent identity Identifying and Utilizing Dependencies Across Cloud Security Services, In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp 133-136, ACM, NY, USA.

[6] Bhadoria RS. Security Architecture for Cloud Computing. In: Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications 2018 (pp. 729-755). IGI Global.

[7] Allenotor, D., Oyemade, D.A and Ojugo, A.A., (2015). A Financial Option Model for Pricing Cloud Compute Resources Based on Cloud Trace Characterization. African Journal of Computing and ICT, Vol. 8, No. 2, Issue 2, Pp 83-92.

[8] Ojugo, A.A., Eboka, A.O., (2014). A social engineering detection model for the mobile smartphone clients, African J. of Computing and ICT, 7(3): pp. 91-100.

[9] Cadregari C., Cutaia, A. (2011). Every Silver Cloud Has a Dark Lining, ISACA JOURNAL Volume 3, pp 1-5.

[10] Creeger, M. (2009). CTO roundtable: Cloud computing. Communications of the ACM 52(8): 50-56.

[11] Khajeh-Hosseini, A., Sommerville, I., Sriram, I., (2010b). Research Challenges for Enterprise Cloud Computing. Submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010.

[12] Fellowes, W. (2008). Partly Cloudy, Blue-Sky Thinking About Cloud Computing. Whitepaper. 451 Group.

[13] Sullivan, T. (2009). "The ways cloud computing will disrupt IT," http://www.cio.com.au/article/296892/nick_carr_ways_cloud_computing_ will_disrupt_it.

[14] Khajeh-Hosseini, A., Greenwood, D., James, J. W., Sommerville, I. (2010a). The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in the Enterprise, Cornell University Library, arXiv:1008.1900 [cs.DC] In: https://arxiv.org/ftp/arxiv/papers/1008/1008.1900.pdf. Accessed: 15th July 2016.

[15] Ojugo, A.A., Otakore, D.O., (2018). Redesigning academic website for better visibility and footprint: a case of Federal University of Petroleum Resources Effurun website, Network & Communication Technologies, 3(1): pp. 33-44.

[16] Babu, G. N. K. S., Srivatsa, S. K. (2014). Security And Privacy Issues in Cloud Computing, International Journal of Engineering, Business and Enterprise Applications (IJEBEA), pp 145-149.

[17] Jensen, M., Schwenk, J., Gruschka, N. and Iacono, L. (2009). On Technical Issues in Cloud Computing. In IEEE International Coference.

[18] Chandra DG, Bhadoria RS. (2012). Role of G-Cloud in citizen centric governance. In2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, (pp. 44-48).

[19] Bhadoria RS, Bansal R, Alexander H. (2011). Analysis of frequent item set mining on variant datasets. Internal Journal of Computer Technology Application, 2(5):1328-33.

[20] Campbell, S., Jeronimo, M. (2006). Applied Virtualization Technology, Hillsboro, OR: Intel Press.

[21] Rongyu, H., Shaojie, W., Jiang, L. (2013). A User-Specific Trusted Virtual Environment for Cloud Computing, Information Technology Journal, 12(10), Asian Network for Scientific Information.

[22] Barham, P., Dragovic, B., Fraser, K. (2003). “Xen and the Art of Virtualization,” ACM SIGOPS Operating Systems Review, vol. 37, no. 5, pp. 164-177.

[23] Smith, S. (2005). Trusted Computing Platforms: Design and Applications, New York: Springer.

[24] Ojugo, A.A., Eboka, A., (2018). Assessing user satisfaction and experience on academic websites: a case of selected Nigerian Universities websites, Int. J. Tech & Comp. Sci., 10(7): pp 53-61.

[25] Scarlata, V., Rozas, C., Wiseman, M. (2008). "TPM Virtualization: Building a General Framework," Trusted Computing, N. Pohlmann and H. Reimer, eds., pp. 43-56, Wiesbaden, Germany: Vieweg Teubner.

[26] Krautheim, F. J. (2009). Private Virtual Infrastructure for Cloud Computing, https://www.usenix.org/legacy/event/hotcloud09/tech/full_papers/krautheim.pdf. Accessed: 30th July 2016.

[27] Jrad, F., Tab, J., Streit, A. (2013). A broker-based framework for multi-cloud workflows, In Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds, pp 61-68, ACM, NY, USA.

[28] Anisetti, M., Ardagna, C. A., Gaudenzi, F., Damiani (2016). A Certification Framework for Cloud-based Services, In Proceedings of the 31st Annual ACM Symposium on Applied Computing, pp 330-447, ACM, NY, USA.

[29] Alqahtani, H. S., Mostefaoui, G. K., Maamar, Z. (2014). A Context-Based Security Framework for Cloud Services, In Proceedings of the 3rd International Conference on Context-Aware Systems and Applications, pp 130-137, ACM, NY, USA.

[30] Islam, S., Weippl. E. R., Krombholz, K. (2014). A Decision Framework Model for Migration into Cloud: Business, Application, Security and Privacy Perspectives. In Proceedings of the 16th International Conference on Information Integration and Web-based Applications & Services. 185-189, ACM, NY, USA.

[31] Sharma, A., Banati, H. (2016). A Framework for Implementing Trust in Cloud. In Proceedings of the International Conference on Internet of things and Cloud Computing, Article No. 6, ACM, New York, USA.

[32] Trabelsi, S., Cerbo, F. D., Gomez, L., Bezzi, M. (2015). A privacy preserving framework for mobile and cloud: a symmetric architecture design, In Proceedings of the Second ACM International Conference on Mobile Software Engineering and Systems, pp 160-161, ACM, NY, USA.

[33] Ojugo, A.A., Yoro, R.E., Eboka, A.O., Yerokun, M.O., Iyawa, I.J.B., (2012). Implementation issues of VoIP to enhance rural telephony in Nigeria, Journal of Emerging Trends in Computing & Information Systems, 4(2): pp. 113-120.

[34] Ojugo, A.A., Abere, R., Orhionkpaiyo, B.C., Yoro., R.E., Eboka, A., (2013). Technical issues for IP-based telephony in Nigeria, Int. J. Wireless Comm. & Mobile Computing., 1(2): 58-67.

[35] Ojugo, A.A., Yoro, R.E., Oyemade, D.A., Eboka, A.O., Ugboh, E., Aghware, F.O., (2013). Robust cellular network rural telephony in Southern Nigeria, American J. of Network Communications, 2(5): 125-132.

[36] Poh, G. S., Nazir, M. A. N. M., Goi, B., Tan, S., Phan, R. C. (2013). An authentication framework for peer-to-peer cloud, In Proceedings of the 6th International Conference on Security of Information and Networks, pp 94-101, ACM, NY, USA.

[37] Youssef, A. E., Alageel, M. (2012). A Framework for Secure Cloud Computing, International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, pp 487-900.

[38] Okonta, E.O., Wemembu, U., Ojugo, A.A., Ajana, D., (2014). Deploying Java platform to design a framework of protective shield for anti-reversing engineering, West African J. of Industrial and Academic Research, 10(1): pp. 50-65.

[39] Ojugo, A.A., Aghware, F.O., Yoro, R.E., Yerokun, M.O., Eboka, A.O., Anujeonye, C.N and Efozia, F.N., (2015). Dependable community-cloud framework for smart mobile-phones, American Journal of Networks and Communications, Vol. 4, No. 4, Pp 95-103.

[40] Oyemade, D.A., Akpojaro, J., Ojugo, A.A., Ureigho, R., Imouokhome, F., Omoregbee, E., (2016). Three tier learning model for universities in Nigeria, J. of Technologies in Society, 12(2): pp. 9-20.