# Using 2x4 Factorial Design to Assess IaaS Delivery Model Security Issues in Heterogeneous Cloud Deployment Models: Case of Selected Firms in Kenya

**Article** · January 2019

CITATIONS
0

READS
36

**1 author:**

Lamek Ronoh
Rongo University
**4** PUBLICATIONS **0** CITATIONS

SEE PROFILE

**Mara Research Journal of Computer Science & Information Security**
**Vol. 1, No. 1, August 2016, Pages 10 - 17**

# Using 2x4 Factorial Design to Assess IaaS Delivery Model Security Issues in Heterogeneous Cloud Deployment Models: Case of Selected Firms in Kenya

Lamek Ronoh
School of Computer Science and Bioinformatics
Department of Information Technology Security
Kabarak University, Private Bag 20157, Kabarak, Kenya
Email: ronohlamek@gmail.com

Received: July 30, 2016
Published: August 5, 2016

**Abstract**

This paper employed the use of a factorial design statistical model to examine and compare cloud security concerns of Infrastructure as a Service (IaaS) service delivery models with their respective deployment models (Private, Public, community and Hybrid clouds). Two companies namely the KenyanCloud and IonaCloud were selected with deployment and service models they use being put into consideration. The objective of the study was to investigate if IaaS delivery service models and the respective deployment model used has a significant effect on cloud computing security concerns in the two selected companies in Kenya. Comparative research design was employed in this study. The significance of the study was to fill the knowledge gap that hitherto not been researched by previous scholars yet it is imperative part as far security of cloud computing is concerned. The findings of this paper hopefully will help the enterprises who intent to embrace IaaS service delivery model when hosted in different deployment models.

**Keywords:** IaaS, Service delivery model, deployment models, private, public, community and hybrid.



## 1.0 Introduction

Most of the enterprises are striving to reduce their computing cost through the means of virtualization. This demand of reducing the computing cost has led to the innovation of cloud computing. Cloud computing is known to offer better computing capability through improved utilization, reduced administration and infrastructure costs. Cloud computing is a natural evolution of the widespread adoption of virtualization, service-oriented architecture and utility computing. Therefore, most of the enterprises are not very confident to adopt it (Savu, 2011).

Rapid adoptions of cloud and ongoing evolutions of technologies and business models creates dynamic services ecosystem which itself is a security risk**.** It is difficult to keep up with the growth of cloud development and forestalling upcoming demands and build a secure cloud. The revolution of cloud computing trends has already begun with the speedy growth of virtualization technology and a rising acceptance of cloud services that combines power of computing capacity, portable devices, web-services and enterprise software, not to mention the utility concept it provide. This behavior not only raises a set of security issues but also makes a new set of legal issues such as compliance and auditing (CCIA, 2009).

Generally, IaaS over the Internet may include services/products such as firewall, networking, Hard disk, RAM, or CPU. It replaces a customer's server room, in-house network staff and network and computers through use of virtualization technology and thus contributes to cost reduction and improved flexibility (Shinder, 2011). More conclusively, Morsy (2010) summarized IaaS possible security risks as follows:

1. **Trusting provider underlying security equipments:** it is difficult for cloud customers to fully understand the provider security configuration in core physical level and also ensuring that the service provider configuration standard does not conflict with customer own organizations security policy.

2. **Identification of appropriate data sources**: it is a challenge to determine which data sources are relevant for incident detection particularly with IaaS (providing intrusion detection for virtual machines without knowing the installed operating system).

3. **Virtual Machine (VM) security**: malware, viruses, DOS, memory leaks and other VM operating system and various workloads are most common security threats. The VM's security is a part of customer responsibility in IaaS.

4. **Security in VM images repository**: unlike physical server, VMs image are still under risk when it is in offline mode. It is common practice to take a snapshot of VMs for disaster recovery. Thus, VM images can be under the risk of malicious codes injection when offline and these VM files could be stolen too. Although, the customer is ultimately responsible for the VM security but since vendor is an owner of the physical hardware there is possibility that cloud provider may copy existing customers VM and reuse for other customers. Another issue in the VM environment is related to VM templates, it is common practice to use templates for rapid deployment of system and all these templates may contain the original owner information which may be re-used for new customers.

5. **Virtual network security**: in IaaS, cloud customers share provider physical infrastructure with many different customers and that increases the risk level of exploiting vulnerabilities in different servers running DHCP, DNS and IP protocols. Virtual Switches (vSwitch) used in IaaS to provide network access to the customer could also be attacked.

6. **Securing VM boundaries**: VM servers can be designed with virtual boundaries (isolated from other VMs) to provide network connectivity among VM servers for security. Generally, VMs co-exist in a physical server to share CPU, memory, network card and other resources. Securing VM boundaries falls under the cloud service provider responsibility, thus misconfiguration and mismanagement could lead to unauthorized access and data leaks.

7. **Hypervisor security**: hypervisor is a 'virtualizer' which map physical server to virtual server. It acts as a central medium of any access to the physical server resources by VMs. Therefore, any compromise on hypervisor means a compromised to hosted VMs. Cloud service provider provides the security of the hypervisor and any vulnerability in hypervisor software inherits security risk in customer VMs.

In Kenyan, for example, in the cloud computing landscape; most enterprises are excited at the idea of embracing cloud computing services. However, majority of such enterprises have little in-depth understanding or knowledge of the security concerns, especially on trade-offs between IaaS service delivery models vis-à-vis the types of deployment used to host it. Hence, this study aims at investigating and analyzing subterranean security issues threatening the cloud computing IaaS service delivery model and its respective deployment models (Private, public, community and hybrid). The paper seeks to identify

the hidden factors existing in these service delivery models that could be accounting for the variation in security of cloud computing architecture.

## STATEMENT OF THE PROBLEM

Infrastructure as a Service (IaaS) is a cloud computing that is a timely idea for enterprises who would want to cut on costs such as storage devices of their ever increasing data, and on hiring maintenance of network staff. IaaS service delivery can be hosted or deployed in either the public, private, community or hybrid models. Nevertheless, no studies have been done to advice the enterprises regarding security trade-offs of the aforementioned deployment models. It is against this backdrop that this paper was written to statistically show the security level model when employed to host IaaS resources. In quest of this, therefore, the paper sought to find out the most critical cloud computing security concerns in IaaS service delivery model and the respective deployment models in the selected firms in Kenya.

## OBJECTIVES OF THE STUDY

The specific objective of the study was to establish whether IaaS service delivery model and the respective deployment models used have a significant effect on cloud computing security in the two selected firms in Kenya.

### Research hypotheses

The hypothesis for the study was stated as follows:

- $H_0$: IaaS service delivery model and the respective deployment models used have no significant effect on cloud computing security in the selected firms in Kenya.

Vs

- $H_1$: IaaS service delivery model and the respective deployment models used at least have a significant effect on cloud computing security in the selected firms in Kenya.

### Conceptual Framework

Figure 1 shows the conceptual framework that guided this study.

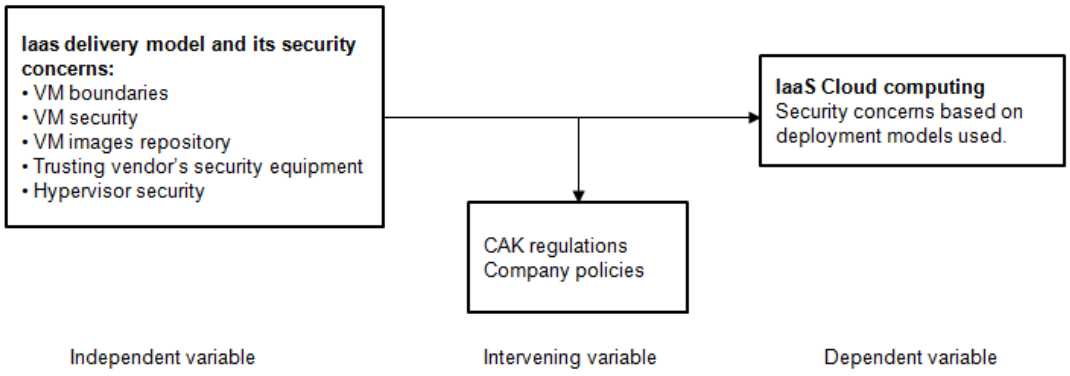


**Figure 1:** Conceptual Framework

Source*:* Researcher

## RESEARCH DESIGN AND METHODOLOGY

Comparative study research design was employed in this study. The goal was to find out why the cases are different and to reveal the general underlying structure which generates or allows such a variation. The comparative method is often used in the early stages of the development of a branch of science. It can help the researcher to ascend from the initial level of exploratory case studies to a more advanced level of general theoretical models, invariances, such as causality or evolution (Routio, 2007).

In comparative analysis, it is imperative and useful to make a factorial table, as shown in Table 1. This design gathered data at a particular point in time with the intention of describing the nature of the existing conditions, identifying the standards against which existing conditions can be compared and determining the relationship that exists between specific events (Kombo & Tromp, 2006). Two levels of IaaS delivery models and four levels of deployment models were compared in a 2x4 factorial asymmetrical shown in Table 1.

**Table 1:** 2X4 Factorial table

| | | Deployment Models | | | |
|---|---|---|---|---|---|
| | | Public | Private | Community | Hybrid |
| (IaaS Delivery model) | Secure | r1,r2 | r1,r2 | r1,r2 | r1,r2 |
| | Insecure | r1,r2 | r1,r2 | r1,r2 | r1,r2 |

Source: Researcher

where $r_1$ and $r_2$ are replications of cloud computing security risks associated with the two selected companies.

The mathematical model for the analysis of factorial experiments was formulated as shown below. The factorial experiment has the effect of two factors, A and B, on the response being investigated. Let there be $n_a$ levels of factor A and $n_b$ levels of factor B. The mathematical model for this experiment was stated as follows:

$$y_{ijk}=\mu_i+a_i+b_j+a_ib_j+\varepsilon_{ijk}$$

where

- $a_i$ is the $i^{th}$ of the effect level of factor **A** ($i=1,2,\ldots,n_a$)
- $b_j$ is the $j^{th}$ of the effect level of factor **B** (($j=1,2,\ldots,n_b$)
- $\mu_i$ is the general constant(Overall effect)
- $a_ib_j$ is the interaction effect between **A** and **B**
- $\varepsilon_{ijk}\sim N(0,\delta^2)$ i.e represents the random error terms( which are assumend to be normally distributed with a mean of zero and variance of $\delta^2$.
- the subscript **k** =1,2,….,m, where m= number of replications

The study was carried out in two selected companies, both located in Nairobi, Kenya dealing with cloud computing services. These two companies were selected using purposive sampling because both have the four cloud deployment models (that is public, private, hybrid and community) and IaaS service delivery models so as to reflect the subject matter that the researcher intends to study and compare.

In order to obtain the subjects for the sample for the two selected companies, Yamane's (1967) formula for calculating the sample size was used.

$$\mathbf{n=N/[1+Ne^2]}$$

where $n$= Sample size, $N$=Population size, and $e$=Sampling error (usually 0.10)

The sample size for each company obtained using Yamane's formula were further divided into homogeneous subgroups (stratum) using stratified random sampling of sample sizes corresponding to groups of respondents used in the study.

## DISCUSSION AND EVALUATION

In order to ascertain whether latent security concerns and trade-offs exists between main or interaction effects of the variables used in this study, factorial analysis of variance (ANOVA) was employed. This design is an inferential statistic which allowed the researcher to test if each of the independent variables have an effect on the dependent variable (hereby called the main effects). The data collected were coded and computed and tabulated in 2x4 factorial design format.

### IaaS delivery model versus cloud deployment models

The results of the factorial design that were generated during analysis included factorial ANOVA table which contains F-value used to reject or accept the null hypothesis based on 5% level of significance and a factorial design graph to check if there is any interaction effect between levels of main factors.

**Table 2:** Between-Subjects factors IaaS levels

| Between-Subjects Factors | | | |
|---|---|---|---|
| | | **Value Label** | **N** |
| **IaaS Security Status** | 1 | Secure IaaS | 8 |
| | 2 | Insecure IaaS | 8 |
| **Deployment model used** | 1 | Private | 4 |
| | 2 | Public | 4 |
| | 3 | Community | 4 |
| | 4 | Hybrid | 4 |

Source:Researcher

Table 3 shows IaaS Factorial ANOVA results.

**Table 3:** ANOVA of IaaS delivery model versus deployment model used

| Tests of Between-Subjects Effects | | | | | |
|---|---|---|---|---|---|
| Dependent Variable:Replication | | | | | |
| **Source** | **Type III Sum of Squares** | **df** | **Mean Square** | **F** | **Sig.** |
| **Corrected Model** | 992.438[a] | 7 | 141.777 | 2.308 | .132 |
| **Intercept** | 2475.062 | 1 | 2475.062 | 40.286 | .000 |
| **IaaS_Status** | .062 | 1 | .062 | .001 | .975 |
| **DeploymentModel** | 27.188 | 3 | 9.063 | .148 | .928 |
| **IaaS_Status * DeploymentModel** | 965.188 | 3 | 321.729 | 5.237 | .027 |
| **Error** | 491.500 | 8 | 61.438 | | |
| **Total** | 3959.000 | 16 | | | |
| **Corrected Total** | 1483.938 | 15 | | | |
| a. R Squared = .669 (Adjusted R Squared = .379) | | | | | |

Source*:* Researcher

The tabulated outcome also indicates the interaction between the main effects between the two models (deployment model * IaaS status (F=5.237, p = .027)).

Furthermore, Figure 2 depicts a high interaction effect between of main factors (IaaS delivery model and deployment models). The resultant graph also strengthens the interaction effects between aforementioned main factors. As can be observed from the graph, private cloud is the safest cloud to deploy IaaS services, whereas public and community clouds are very insecure clouds as far as IaaS service delivery in the cloud is concerned. Since the P-values for main interaction effects between deployment models and Saas security status effects are (F=5.237, p = .027<0.05), we reject $H_0$ at 5% level of significance and conclude that IaaS service delivery model and the respective deployment models used have significant effect on cloud computing security in the selected firms in Kenya.

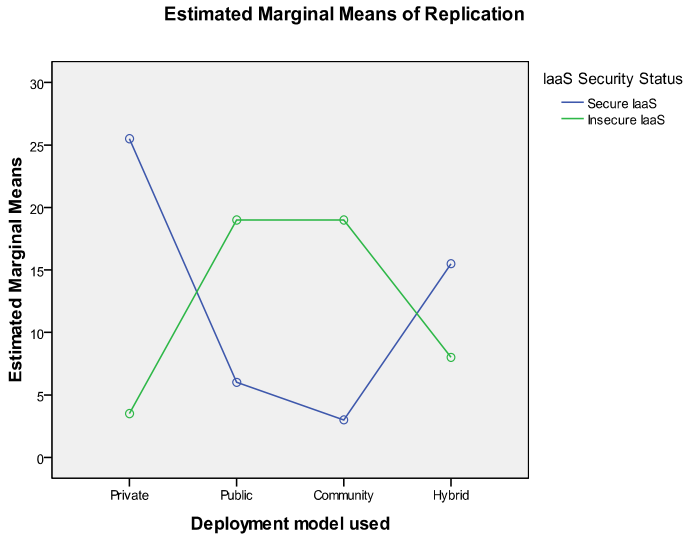


**Figure 2:** A graph depicting interaction effect between IaaS delivery model and cloud deployment models
Source: Researcher

## CONCLUSION

The findings of the study have indicated that the kind of deployment model used as a mode of provisioning the cloud computing IaaS delivery models matters a lot because it has a considerable impact on the security concerns. More particularly, it was observed that the private cloud is the safest and trustworthy cloud to deploy IaaS over cloud. The hybrid cloud came second though a distant far from private cloud. It was further observed that public and community clouds are equally a risky model for deploying IaaS. The companies offering cloud computing services here in Kenya are aware of the risks but not from this perspective. The outcome of this research paper hopefully gives inkling on latent parameters affecting IaaS service delivery model when hosted in different deployment models.

## RECOMMENDATIONS

The recommendations made in this study are expected to assist in minimizing risks involved when choosing and deploying cloud computing services. Having looked at the findings of security concerns on the SaaS service delivery model vis-à-vis the type of deployment model used, the study recommends the following:-

(i) While choosing the service delivery model, it is imperative to also decide on the type of deployment model one should use in the cloud.

(ii) Besides private cloud, clients should embrace hybrid deployment model because it leverages the advantage of the other cloud models, providing a more optimal user experience.

(iii) The factorial design approach of analyzing cloud computing security is expected to give an insight to providers who should come up with a new model of delivering and deploying cloud computing services to clients. The model should offer enhanced choice, flexibility, operational efficiency and safety of the customer.

## REFERENCES

CCIA (2009). Abstract*: Cloud Computing, Computer & Communications Industry Association.* Retrieved on August 30, 2012 from http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000151/Cloud_Computing.pdf

Kombo, D.K. and Tromp D.L.A.(2006). *Proposal and Thesis Writing,an Introduction*, Nairobi: Paulines Publishers.

Kothari C.R. (2004). *Research Methodology, Methods and Techniques, (*2nd ed.). New Delhi: New Age International Publishers.

Morsy A. M., Grundy J., Muller I.(2010). *An Analysis of The Cloud Computing Security Problem.* Retrieved October 25, 2012 from http://www.ict.swin.edu.au/personal/malmorsy/Pubs/cloud2010_1.pdf

Rehan, S.(2011). *Cloud computing's effect on enterprises*. Unpublished master's thesis, Lund University.

Routio, P.(2007). *Comparative Study*. Retrieved on August 3rd, 2012 from http://www2.uiah.fi/projects/metodi

Savu, L.(2011).*Cloud Computing: Deployment Models, Delivery Models, Risksand Research Challenges*. Tirunelveli, IEEE.

Shinder T.W. (2011, August 3). Security Issues in Cloud Deployment model. *TechNet Articles*, p. 2. Retrived on August 3rd , 2012 from http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud-deployment-models.aspx from TechNet database .

Yamane, T.(1967). *Sampling Statistics*. New Jersey(Englewood Cliffs): Prentice-Hall.

*Cite this article:*

Ronoh, L. (2016). Using 2x4 Factorial Design to Assess IaaS Delivery Model SecurityIssues in Heterogeneous Cloud Deployment Models: Case of Selected Firms in Kenya. MR Journal of Computer Science & Information Security. Vol. 1, No. 1, pp. 10 - 17.