ISSN No:-2456-2165

A Descriptive Research on the Security Challenges of Cloud Computing Among Selected SMEs in Kenya

Dr. Satwinder Singh Rupra

Abstract:- Cloud computing can help organizations accomplish more by paying less and breaking the physical boundaries between IT infrastructure and its users, however heightened security threats must be overcome in order to benefit fully from this new computing exemplar. The objective of this research was to determine the fundamental cloud security challenges experienced by SMEs in Kenya. Descriptive survey was therefore chosen for this study because the researcher was interested in the opinions of the respondents in terms of security challenges in cloud computing. The primary area of study for this research was Nairobi, Kisumu and Mombasa and the target population for this study were the Top 100 SME companies in Kenya as of 2016. This information could be useful and vital to policy makers and researchers who are making efforts to improve security in the field of Cloud Computing.

I. INTRODUCTION

Cloud computing can help organizations accomplish more by paying less and breaking the physical boundaries between IT infrastructure and its users, however heightened security threats must be overcome in order to benefit fully from this new computing exemplar (Palmer, 2015). It is noted that mid-sized businesses which include SMEs, focus their investment on customer satisfaction and mechanisms of reducing operating costs and therefore tend to disregard necessary investment towards securing their cloud infrastructure (Khajeh, Greenwood, Smith, & Sommerville, 2012). Therefore, they become more vulnerable than larger organizations that have dedicated budgets and personnel to handle their IT infrastructures.

The cloud computing service models and their typical uses are illustrated in Figure 1:

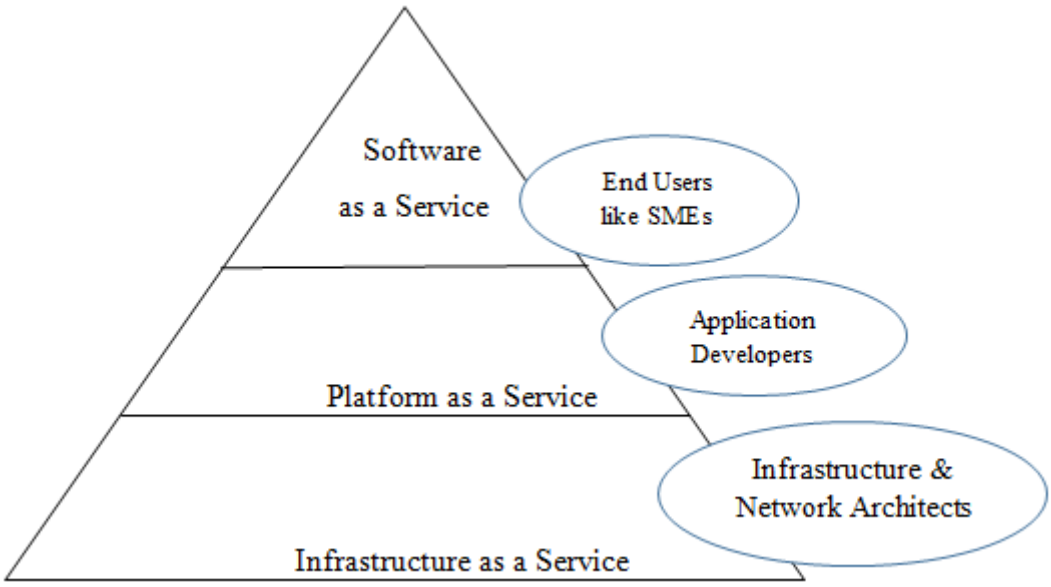

Fig 1:- Cloud Computing Service Models
Source: *Author (2020)*

➢ *Objective*

The objective of this research was to determine the fundamental cloud security challenges experienced by SMEs in Kenya. This information could be useful and vital to policy makers and researchers who are making efforts to improve security in the field of Cloud Computing. To do this, SMEs from manufacturing, hospitality, health and finance sectors were surveyed using questionnaires and strategically interviewed on various SaaS cloud security challenges. The key factors which influence vulnerabilities were identified, including people, lack of technologies and external factors like cloud provider regulations. The quantitative data was analysed using descriptive statistics. The descriptive statistics was used to describe and summarize the data in form of graphs, tables, charts, frequencies and percentages. For the qualitative data a thematic analysis approach was used. The Statistical Package for Social Sciences (SPSS) version 20 was used to analyse the data.

II. ASSUMPTIONS

The study was based on the following assumptions

- That all participants responded accurately and honestly regarding their cloud computing security.
- That the selected sample for the study was a representative of the population to which references were made.
- That the scales used for data collection yielded valid and reliable information for answering the research objectives and questions.

➢ *Research Design*

Oso and Onen (2011) have described a research design as a plan on how the researcher intends to conduct the research while Donald and Delno, (2006) have also noted that a research design is a framework of how data was collected and analysed in an investigation. Research design therefore provides the most valid and accurate answers to research questions.

This study adopted descriptive research designs. Descriptive research is a study designed to depict the participants in an accurate way and describes people who took part in this study (Kowalczyk, 2015). This approach assisted the researcher to analyse and define the security of SaaS cloud computing among the top 100 SMEs in Kenya. This involved using a questionnaire to collect views of staff in the SMEs.

Descriptive survey was therefore chosen for this study because the researcher was interested in the opinions of the respondents in terms of security challenges in cloud computing. Descriptive research design enabled the researcher to generalize the findings to a larger population. The research in this case generalized the security challenges of cloud computing among SMEs in Kenya. In addition, the study adopted a mixed method approach in which both qualitative and quantitative data were collected. Combining both quantitative and qualitative data enabled the researcher to best understand and explain a research problem (Creswell, 2014).

This procedure seemed to capture the complexity of SMEs of their workplace conditions. Therefore, a combination of quantitative and qualitative research was a better option. Interviews assisted in achieving a more behaviourally related assessment of the participants' lives at work and a better indication of the exact factors that contributed to their levels job dissatisfaction (George, Louw & Badenhorst, 2008).

➢ *Location of Study*

The primary area of study for this research was Nairobi, Kisumu and Mombasa as shown in Table 1. These three cities were selected for the study as they inhibit the major share of SMEs that utilize IT resources for infrastructure growth. The cities are also well connected in terms of internet increasing the rates of SaaS cloud computing adoption as compared to smaller towns. This makes it suitable for conducting research on cloud computing security.

The SMEs were selected using purposive sampling technique so that the researcher can reflect the subject of the matter that needs to be studied. Purposive sampling is a sampling method where the sample is selected based on characteristics of a population and the objective of the study.

➢ *Population of the Study*

A population refers to a group of individual persons, objects or items from which samples are taken for measurement (Creswell, 2014). The target population for this study was the Top 100 SME companies in Kenya as of 2016. This target population was chosen purposively for this research because these companies have sensitive and crucial data that needs to be kept secure and private as well as utilize IT resources for infrastructure growth. The companies consist of those in the manufacturing, hospitality, health and finance sectors and are currently using cloud computing or considering the use of cloud computing due to their infrastructure size and requirement. The SMEs had people participating in the research that filled in the questionnaire. These included the directors or CEOs, finance in charge, IT administrators and data/system users. Finally, the sample population of SMEs are selected to meet the following criteria:

- SMEs with number of employees not exceeding 250;
- SMEs must be in Kenya;
- SMEs must use the cloud computing for business data storage and/or operations;
- SMEs must have at least one employee in charge of ICT or technical operations or a chief-level officer responsible for operations.

➢ *Sampling Techniques and Sample Size*

Sampling procedure refers to the process and function of selecting a sample that represent a given population. In order to determine the sample size of SMEs to be drawn from the 100 SMEs in the study area, the study adopted a formula from Nassiuma (2000) using the coefficient of variation for estimating a sample size, n, from a known population size, N.

$$n = \frac{NC^2}{C^2 + (N - 1)\, e^2}$$

Where n= sample size
N= population, 100 SMEs in this case.
C= Co-efficient of variation, assumed to be 22%.
e = Standard error, assumed to be 0.02 in this case.

Therefore, $n = \frac{100 \times 0.22^2}{0.22^2 + (100-1)\, 0.02^2}$

n=16.388 (rounded off to 16)

For the purpose of this study, 16 companies were sampled under different sectors which included manufacturing, hospitality, health and finance sectors. The SMEs were selected using purposive sampling from the areas as shown in Table 1.

City	No. of SMEs from top 100	Sample Size
Nairobi	80	9
Kisumu	9	5
Mombasa	7	2
Rest of Kenya	4	0
Total	**100**	**16**

Table 1:- Sampling Frame
Source: *Author (2019)*

Purposive sampling technique was used to sample the 16 SMEs that had the characteristics the researcher was looking for; having sensitive and crucial data that needs to be kept secure and private as well as utilize IT resources for infrastructure growth. The choice of purposive sampling technique is prompted by assertion that purposive sampling is one in which persons are deliberately selected for the vital information they can make available that cannot be obtained from other choices (Padgett, 2016). The Rest of Kenya depicts smaller towns and these were not included in the sample size but are illustrated on Table 2 for understanding purposes.

Members of SMEs who were selected to participate in the study were those that were directly involved with data and decision making of the SMEs. From each of the 16 sampled SMEs 15 people were purposively selected to participate in the study. Therefore, the sample size used in this study was 240 respondents. The distribution is as shown in Table 2.

Department	Number of respondents	Total number of respondents
Directors/Owner/CEO	1	16
Finance controller	1	16
Accounts department	3	48
IT admins/technicians/IT staff	5	80
Data user/ System user	5	80
Total	**15**	**240**

Table 2:- Members of SMEs participating in the Questionnaire
Source: *Author* (2019)

- *Questionnaire Design*

The questionnaire was structured and mainly self-completion in nature; that is, the respondents were required to answer the questions themselves unaided (independently). The study adopted and administered a set of mixed closed ended questions. Though the questions were the closed-ended type, in few instances it was necessary to ask for the respondents for their independent opinions.

➢ *Reliability and Validity Analysis*

According to Creswell (2014) reliability of an instrument is the measure of the degree to which a research instruments yields consistent results or data after repeated trials. Thus, reliability refers to consistence of measurement of the magnitude to which the results are similar over different times of data collection and the extent to which the measures are free from error.

Oso & Onen (2011) observe that in investigating test reliability of research questionnaire several methods such as; test-retest reliability, split-halves, parallel forms and internal consistency can be used. Internal consistency measures consistency within the instrument and questions how well a set of items measures a particular behaviour or characteristic within the test.

According to Oso & Onen (2011), the most popular method of testing for internal consistency of a Likert-scale-itemed questionnaire is Cronbach's alpha coefficient. It's the most standardized test of inter-item consistency reliability. It defines the degree to which an instrument is error free, reliable and consistent across the various items in the scale. Hence, the Cronbach's alpha coefficient test was used to measure the internal consistency of the questionnaire in this study.

Scale	No. Items	Cronbach's alpha	Cronbach's alpha based on standardized items
Security Challenges	8	.783	.811
Security Measures	8	.623	.578
Concerns on Cloud Computing	7	.712	.698

Table 3:- Internal Consistency: Cronbach's Alpha Results for the Questionnaire
Source: *SPSS Analysis.*

Table 3 revealed that all the sub-scales met the required level of internal consistency of reliability, with the Cronbach's alpha values ranging from a low of 0.623 (security measures items) to a high of 0.783 (security challenge). These findings were in line with the rule of thumb proposed by Frankel & Wallen (2009) that; a coefficient of 0.60 is an average reliability while coefficient of 0.70 and above indicates that the instrument has a high inter-item consistency reliability standard.

The Cronbach's alpha for all the sub scales revealed that the questionnaire had adequate reliability for the study. Deleting any of the items in the sub-scales would not result to further increase in Cronbach's alpha, that is, it would not cause improvement in the internal consistency. It was also noted that all items correlated with the total scale to a good degree. Hence, the questionnaires was generally suitable for data collection because they adequately measured the constructs for which they were intended to measure.

Internal validity of the constructs was tested by subjecting the survey data to suitability tests using the Kaiser-Meyer-Oklin measure of sampling adequacy (KMO Index) and the Bartlett's Test of Sphericity. This internal validity of the constructs was tested for each sub-scale, as summarized in Table 4.

Subscale	Kaiser-Meyer-Olkin (KMO index)	Bartlett's Test of Sphericity		
		Approx. Chi-Square	df	Sig.
Security Challenges	.714	330.715	15	.000
Security Measures	.734	278.234	15	001
Concerns on Cloud Computing	.842	351.351	15	.000

Table 4:- KMO and Bartlett's Test of Internal Validity
Source: *Survey data (2018), SPSS Analysis*

From Table 4, the value of Bartlett's test of Sphericity is significant ($p \leq 0.001$) for all the sub-scales of the questionnaire. In addition, the Kaiser-Meyer- Olkin indexes are all > .6 which is a threshold for a sufficient internal validity. Creswell (2014) asserts that if the Bartlett's test of Sphericity is significant, and if the Kaiser-Meyer-Olkin measure is greater than 0.6, then condition of adequate internal validity is met. Given the results of the validity tests met these conditions, it implies that questionnaire was of required validity levels and data collected were suitable for inferential analysis.

III. RESEARCH OUTPUTS

- *Security Challenges in Deployment Models*

The views of the respondents on security challenges faced in SaaS delivery model in their respective deployment models were collected using eight itemed Likert scaled questionnaire. The items were rated using strongly Agree=5, agree=4, Undecided=3, Disagree=2 and strongly disagree=1. The views of the respondents were summarized in percentage frequencies, as shown in Table 5.

Item	SA	A	U	D	SD	M	Std. Dev
Data/information stored on the cloud may face a lot of availability issues due to	78 (38.6%)	66 (32.7%)	28 (13.9%)	24 (11.9%)	6 (3.0%)	3.92	1.12
A cloud administrator may become a very high risk if they turn rouge and try and access data stored on clouds.	74 (36.6%)	74 (36.6%)	30 (14.9%)	14 (6.9%)	10 (5.0%)	3.93	1.11
Whenever the data owner makes a command to delete a cloud resource, there is no certain way of telling that the data has been deleted to its entirety.	36 (17.8%)	68 (33.7%)	50 (24.8%)	26 (12.9%)	22 (10.9%)	3.35	1.22
Because the owner of the data has not control over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way.	56 (27.7%)	58 (28.7%)	42 (20.8%)	38 (18.8%)	8 (4.0%)	3.57	1.19
In SaaS model, hackers can manipulate weakness in data security model to get an illegitimate access to data or application.	44 (21.8%)	76 (37.6%)	48 (23.8%	26 (12.9%)	8 (4.0%)	3.60	1.08
Cloud computing creates lack of liability of providers in case of security incidents.	32 (15.8%)	58 (28.7%)	32 (15.8%)	48 (23.8%)	32 (15.8%)	3.05	1.34

Multi-tenancy in the cloud a major issue for clients due to the possibility of a hacker taking advantage of the same host.	48 (23.8%)	62 (30.7%)	47 (23.3%)	28 (13.9%)	17 (8.4%)	3.49	1.22
Password protection in itself is enough to secure against unauthorized access in the cloud.	32 (15.8%)	58 (28.7%)	21 (10.4%)	56 (27.7%)	35 (17.3%)	2.99	1.37
Mean average response on security challenges						3.49	0.69

SA-strongly agree, A-agree, N-neutral, D-disagree, SD-strongly disagree, M-mean and Std.Dev.-Standard deviation.

Table 5:- Respondents Views of on Security Challenges

Source: *Survey data (2017)*

The findings of the study revealed that Cloud computing face considerable security and related challenges in the implementation of SaaS delivery model. This was reflected by mean average response rate of 3.49 with standard deviation of 0.69, on the rating scale of 1 to 5. All the items were rated above mean score of 2.5; ranging from a minimum of 2.99 to a maximum of 3.93.

This finding affirms the assertion of Shroff (2010) that since cloud computing is not a standalone computing platform because it combines several technologies including networks, operating systems (OS), databases, virtual servers and components, resource scheduling, transaction processing, concurrency control techniques, load balancing, memory management and numerous others for its functionality and operation, a threat in any one of the technologies becomes a threat for the entire cloud platform. This causes a serious security challenge in the implementation of SaaS delivery model.

At a mean response rate of 3.92 (Standard deviation=1.12) a significant majority of 144 translating to 71.3% of the respondents observed that data/information stored on the cloud may face a lot of availability issues due to downtime in the internet. They pointed out that many regions face challenges with stable and affordable internet connections yet all the data, resources and applications are only accessible through the internet. Only 32 (14.9%) of them were on the contrary opinion that cloud face a lot of availability issues due to downtime in the internet.

In support to this finding is Omwansa, Waema and Omwenga (2014) whose findings had established that downtime is a major disadvantage of cloud computing especially in evolving countries. They had pointed out that since all the data, resources and applications are only accessible through the internet, an internet outage means users have no access to them.

Similarly, the findings of the study established that a cloud administrator may face a very high risk if they turn rouge and try and access data stored on clouds. This point of view was reflected by a mean average score of 3.93, with nearly three quarters 148 (73.2%) of the IT staff who were engaged in this study agreeing that a cloud administrator may be exposed to high risk if they turn rouge and try and access data stored on clouds.

In addition, it emerged that cloud computing is faced with a lack of certainty in trailing actions of the users. For example, although 50 (24.8%) of respondents remained non-committal, more than a half 104 (51.5%) of them confirmed that whenever the data owner makes a command to delete a cloud resource, there is no certain way of telling that the data has been deleted to its entirety. This means that there is no sure way of confirming that documents or personal data on the cloud has been successfully deleted by the user.

This finding agrees with Behl (2011) who observed that since most cloud platforms are hosted off-site, an organization is not able to have full control over the hardware, technology and backend details of the cloud platform. Customarily, when an organisation outsources their data and services to a cloud vendor, users are not aware and have no control over the location of their data, which is a serious concern to a user perspective; organizations lose control over their vital data and are not aware of any security mechanisms put in place by the provider.

Equally, Pearson and Benameur (2010) had noted that user-centric control is not possible with the cloud because the vendor acquires full responsibility for storage of data as soon as a SaaS cloud infrastructure is used, hence users lose visibility and control over it. In the cloud archetype, users' data is handled in 'the cloud' on hardware, software and platform the users do not own or control and therefore it becomes a threat in terms of theft.

On the same note, the study revealed that legality of the data in the cloud is not easy to voucher. Majority 114 (56.4%) of respondents, translating to a mean score of 3.57, were of the general feeling that since the owner of the data does not have control over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way.

The respondents observed that it is not clear that it is possible for a cloud provider to ensure that a data owner can get access to all their data including metadata and system related files. It is also difficult to get data back from the cloud, and avoid vendor lock-in. Equally, nearly six out of ten 120 (59.4%) of the respondents observed that in SaaS model, hackers can manipulate weakness in data security model to get an illegitimate access to data or application.

These findings agree with the position held by Pearson and Benameur (2010) that loss of visibility and control of the data by the consumer in cloud computing may cause risk of misuse, especially for different purposes from those originally notified to and agreed with the consumer, or unauthorized resale.

Similarly, this finding is in line with the argument held by Khan and Malluhi (2010) that data entrusted to different systems and platforms located in different locations, managed by unknown users, and regulated by the laws of other countries cannot be fully be relied on without fear of abuse, loss of confidentiality, integrity and availability of data.

They observe that a consumer does not know whether the security profiles of the remote locations are the same as what they have in-house or whether the regulatory compliances like HIPAA hold in all the locations, does not know who can access the data stored on various disks in multiple locations.

The findings of the study show that multi-tenancy in the cloud is a major issue for clients due to the possibility of a hacker taking advantage of the same host. This was revealed by more than a half 110 (54.5%) of the IT staff who took part in the study and reflected by a mean response rate of 3.49, with a standard deviation of 1.22.

The respondents observed that when a multi-tenancy has been achieved, an attacker takes advantage of the system characteristics to hack other users' data. They further argue that the risk from for such attacks is high because they cannot be detected by the hypervisor or the operating system.

This finding concurs with Jahdali *et al*, 2014) who had postulated that because multi-tenancy in cloud computing is unique in a way that both the attacker and the victim are sharing the same servers, the setup cannot be countered by native security measures and controls because they are not designed to secure inside the servers and they are limited just to the network layer.

Equally, Sen and Sengupta (2005) observed that security challenge is the biggest question that arises to the managements of any organization that wants to move to the cloud. They reiterate that threats and flaws in technologies like operating systems, virtual platforms, transaction processing systems, and concurrency control procedures and the likes form part of the cloud security issues.

On the contrary, the findings of the study show a sharp division on opinion on whether or not there is lack of liability in case of security incidences as a result of cloud computing. Although, 90 (45.5%) of the respondents held a strong opinion that cloud computing creates lack of liability of providers in case of security incidents, almost equal proportion 80 (39.6%) of the surveyed IT staff refuted the assertion that cloud computing creates lack of liability of providers in case of security incidents.

Similarly, whereas 32 (15.8%) of the respondents strongly believed that password protection in itself is enough to secure against unauthorized access in the cloud, 35 (17.3%) of them held that password protection in itself is not adequate to secure against unauthorized access in the cloud. They claim that some people may misuse existing privileges to gain further access or support third parties in accesses data/information they are not meant to access, this infers with the confidentiality and integrity of information within the cloud service. This finding of the survey is line with the argument by Saripalli and Walters (2010) that by spending a little money to buy cloud space, an attacker has a considerable chance to allocate his VM next to the victim's VM the potential attacker is able to take advantage of the system characteristics to hack breach the victim's data and such attack cannot be easily detected by the hypervisor or the operating system.

- *Security Measures Provided by Cloud Provider*

The study sought to investigate the sufficiency of security measures provided by cloud provider to cater for all the areas of cloud computing that need to be secured. The views of the respondents on sufficiency of security measures were gathered using eight itemed Likert scaled questionnaire.

The constructs of the items were based on possible indicators of security measures towards various areas of cloud computing. The items were to be rated using 5=Very sufficient, 4=largely sufficient, 3=Somehow sufficient, 2=largely insufficient and 1=Very insufficient. The views of the respondents were summarized in percentage frequencies, as shown in Table 6.

Item	5	4	3	2	1	Mean	Std Dev.
Cloud computing supplier maintains proper security monitoring logs of all access to your data and documents access as routine, random audit, or suspicious leveraging their prescribed scripts and operational procedures as the basis for all audit in all deployment models.	74 (36.6%)	72 (35.6%)	40 (19.8%)	10 (5.0%)	6 (3.0%)	3.98	1.01
User access control rules, security policies and enforcement are made available to the customer in a well-informed manner.	76 (37.6%)	102 (50.5%)	18 (8.9%)	6 (3.0%)	0 (0.0%)	4.23	0.73
In SaaS, applications are multi-tenant hosted by 3rd party usually exposes functionality could result multifaceted security issues.	48 (23.8%)	84 (41.6%)	50 (24.8%)	14 (6.9%)	6 (3.0%)	3.76	0.99
Cloud computing providers provide sufficient security for data at rest. (Stored data in the cloud).	50 (24.8%)	80 (39.6%)	44 (21.8%)	22 (10.9%)	6 (3.0%)	3.72	1.04
Cloud computing providers provide sufficient security for data in transit. (Data being transferred from the cloud to the user computers and vice versa).	46 (22.8%)	76 (37.6%)	58 (28.7%)	20 (9.9%)	2 (1.0%)	3.71	0.96
Cloud computing providers provide sufficient authentication platform for users to access the cloud.	38 (18.8%)	96 (47.5%)	52 (25.7%)	10 (5.0%)	6 (3.0%)	3.74	0.92
Cloud providers have sufficient and credible policies and practices especially for things like data retention, deletion and security.	40 (19.8%)	82 (40.6%)	48 (23.8%)	28 (13.9%)	4 (2.0%)	3.62	1.01
Customers understand how incidents and disasters will affect their data and therefore have relevant recovery procedures for the same.	24 (11.9%)	54 (26.7%)	60 (29.7%)	36 (17.8%)	28 (13.9%)	3.05	1.21
Mean average response rate on sufficiency of security measures						3.73	0.98

5-Very sufficient; 4-Largely sufficient; 3-somehow sufficient; 2-largely insufficient; 1-very insufficient; M-mean and Std. Dev.-Standard deviation

Table 6:- Views of Respondents on Security Measures
Source*: Survey data (2017)*

Table 6 indicates that members that were directly involved with the data and decision making of the SME who took part in the survey rated, as largely sufficient (average score=3.73; standard deviation=0.98), in the scale of 1 to 5 of sufficiency of security measures provided by cloud providers to cater for most of the areas of cloud computing that need to be secured.

All the indicators were rated above 3.00, with "user access control rules, security policies and enforcement" receiving the highest rating (mean average score=4.23; standard deviation=.73). Nearly nine out of ten 176 (88.1%) of the respondents held a general feeling that user access control rules, security policies and enforcement are made available by the cloud providers to the customer in a well-informed manner. Sen and Sengupta (2005) had observed that cloud technologies be secure enough to provide for overall security of the system; the network between the end users and the cloud infrastructure needs to be secure, data at rest also needs to be secure by encrypting the data and enforcing relevant policies for data sharing and resource distribution and memory management systems need to be secured.

Similarly, although some 32 (15.9%) of the respondents held a contrary opinion, majority 122 (60.4%) of them observed that cloud providers have sufficient and credible policies and practices especially for things like data retention, deletion and security. Those who held contrary opinion argue that policies and practices on issues like data retention, deletion and security are insufficient and not adequate to address security challenges. They felt that

ISSN No:-2456-2165

some customers hardly ever have their legal and regulatory experts inspect cloud provider policies and practices data retention, deletion and security.

It emerged that more than seven out of every ten 146 (72.3%) of the SMEs staff sampled for the survey, reflecting a mean average score of 3.98 (standard deviation=1.01), were in agreement that cloud suppliers maintain proper security monitoring logs of all access to their data and documents access as routine, random audit, or suspicious leveraging their prescribed scripts and operational procedures as the basis for all audit in all deployment models.

However, some 16 (8.0%) of them said cloud computing suppliers do not sufficiently maintains proper security monitoring logs of all access to their data and documents access as routine, random audit, or suspicious leveraging their prescribed scripts and operational procedures as the basis for all audit in all deployment models. They also observed that some cloud vendors also usually do not allow clients to carry out audits, meaning that certain kind of compliances cannot be achieved.

On multi-tenant, the findings of the study show that although a sizeable proportion 50 (24.8%) of the respondents remained non-committal, many 132 (65.3%) of them were in agreement that in SaaS, applications that are multi-tenant hosted by 3rd party usually expose functionality that could result in to multifaceted security issues. Likewise, despite the fact that 78 (38.6%) of the sampled staff of SMEs agree that customers of cloud computing understand how incidents and disasters affect their data, 64 (31.7%) of them alluded that cloud computing suppliers lack relevant recovery procedures for such data. This was reflected by a mean average score of 3.05, with standard deviation of 1.21.

On the sufficiency of security measure on data, many 130 (64.4%) of the study participants were contented that cloud computing providers provide moderately sufficient security for data at rest/ stored data in the cloud, translating to a response rate of 3.72 (std. dev.=1.04). On the other hand, some 28 (13.9%) of the respondents believed that there is insufficient security of such data, while 44 translating to more than a fifth (21.8%) of respondents also remained doubtful on the security of data in the cloud.

Equally, it came out clearly that despite the fact that a majority of 122 (60.4%) of the sampled staff were of the general agreement that cloud computing providers provide sufficient security for data in transit, about a tenth 22 (10.9%) of them insisted that the providers do not provide sufficient security for the data being transferred from the cloud to the user computers and vice versa. Interestingly, more than one out of every four 58 (28.7%) of those who were directly involved with the data and decision making of the SME who took part in the survey were not aware of security concerns of data in transit and how the cloud computing providers handle the matter.

This was despite the fact that CPNI Security Briefing (2010) had pointed out that cloud vendors should come up with different technologies and standards to increase their security but then the customers to ensure that security in the cloud meets their own security requirements and policies. They suggest that both vendors and users should carry out risk assessments and due diligence of the cloud security models.

The results of the survey also revealed that there was differing opinion from the staff directly involved with the data and decision making of the SME on provision of authentication platform. This was revealed by the fact that whereas, 38 (18.8%) of the staff sampled for the survey strongly believed that cloud computing providers provide sufficient authentication platform for users to access the cloud, some 16 (8.0%) of them held a contrary opinion.

These respondents believe that cloud providers sometimes do not provide users with strong user access control to access data so as to keep off unwanted users. However, 52 (25.7%) of the respondents said that although there is some authentication platform for users to access the cloud, it is only somehow sufficient.

- *Concerns in Cloud Computing in Deployment Models*

The views of the respondents on concerns on cloud computing in SaaS deployment models were gathered from members that were directly involved with the data and decision making in the SME. Their views were gathered using eight itemed Likert scaled questionnaire on the main concerns in their approach to cloud computing. The items were to be rated using: Not Important at all=1; Slightly Important=2; Somewhat Important=3; Largely Important=4 and Very Important=5. The views of the respondents were summarized in percentage frequencies, as shown in Table 7.

Item	1	2	3	4	5	M	Std Dev.
Privacy	24 (11.9%)	14 (6.9%)	4 (2.0%)	24 (11.9%)	136 (67.3%)	4.16	1.42
Availability of services and/or data	18 (8.9%)	16 (7.9%)	8 (4.0%)	32 (15.8%)	128 (63.4%)	4.17	1.33
Integrity of services and/or data	16 (7.9%)	16 (7.9%)	8 (4.0%)	24 (11.9%)	138 (68.3%)	4.25	1.30
Confidentiality of corporate data	24 (11.9%)	8 (4.0%)	6 (3.0%)	34 (16.8%)	130 (64.4%)	4.18	1.37
Loss of control of services and/or data	14 (6.9%)	20 (9.9%)	12 (5.9%)	58 (28.7%)	98 (48.5%)	4.02	1.25
Lack of liability of providers in case of security incidents	14 (6.9%)	24 (11.9%)	30 (14.9%)	60 (29.7%)	74 (36.6%)	3.77	1.25
Inconsistency between trans national laws and regulations	18 (6.9%)	22 (11.9%)	40 (14.9%)	56 (29.7%)	66 (36.6%)	3.64	1.28
Intra-clouds (vendor lock-in) migration	14 (6.9%)	26 (11.9%)	30 (14.9%)	68 (29.7%)	64 (36.6%)	3.70	1.23
Mean average score on concerns on cloud computing						3.99	1.30

1=Not Important at all; 2=Slightly Important; 3=Somewhat Important; 4=Largely Important; 5=Very Important; M=mean score and Std. Dev.= Standard Deviation.

Table 7:- Views of the Respondents on Concerns on Cloud Computing

Source: *Survey data (2017)*

Table 7 reveals that people directly involve in data and decision making in the top 100 SMEs organizations in Kenya generally feel that concerns on cloud computing are largely important. This was reflected by a mean average score of 3.99 (standard deviation=1.30), with most of the concerns rated as very important (mean score rating > 4.00). Concern on integrity of services and/or data received the highest rating (mean=4.25), with over four fifth 162 (80.2%) of the respondents indicating that concern on integrity of services or data is quite important in regard to cloud computing.

Stallings and Brown (2008) had observed that cloud computing provider is entrusted by their clients to provide integrity for their data but due to the working nature of the cloud model, several threats including complicated insider attacks can take place. Malicious employee can intentionally fabricate a program to fail when a certain command is executed or a certain time is reached. Moreover, the security of cloud services is reliant on the security of the API or interfaces that the cloud providers offer to their customers, thus if unauthorized users gain control of interfaces, data integrity can be seriously violated.

Equally, concerns on privacy was rated very high, as reflected by a mean rating score of 4.16 (standard deviation =1.42) with a significant majority 160 (79.2%) of the respondents asserting that privacy of data and services in quite important in cloud computing. In addition, the findings of the study show that confidentiality of corporate data is very important (mean score = 4.18) and key in cloud computing, with nearly two thirds 130 (64.4%) of rating it as of very high importance.

This finding concurs with the views held by Modi, Patel, Borisaniya, Patel and Rajarajan (2013) that unauthorized right of entry may take place due to an application vulnerability or weak identification, increasing chances of confidentiality and privacy breaches. However, they asserted that the cloud provider is responsible for providing secure cloud instances, which should ensure users privacy. Similarly, Zissis and Lekkas (2012) portends that because the cloud allows many access points for its users to connect (usually from anywhere with internet access), authorization is crucial to maintain data integrity and security at large.

It was established that a significant majority of 160 translating to 79.2% of the respondents were in general agreement that availability of services and/or data in cloud computing is of a very important concern (mean score=4.17) to the users. On the same note, it emerged that loss of control of services and/or data is equally another important concern in cloud computing. This was revealed by nearly a half 98 (48.5%) of study participants who strongly observed that since most cloud platforms are hosted off-site, their organization does not have full control over the hardware and technology. In addition, most of the study participants held that since cloud computing involve outsourcing of data and services to a cloud vendor, the users are not aware and have no control over the location of

their data, which is a very serious concern, as reflected by a mean score of 4.02.

On the flip flop, the study findings revealed that although issues of security incidents is a concern to many 134 (66.3%) users of cloud computing, a considerable proportion 38 (18.8%) of the respondents observed that issues of security incidents is not a serious concern. However, majority of the respondents held that there is lack of liability of providers in case of security incidents. Some of the respondents were concerned that customers are sometimes never made to understand how incidents and disasters affect their data.

However, the findings of the study established that although there is concern about inconsistency between transnational laws and regulations, it is not very serious as reflected by a mean score of 3.64 (standard deviation=1.28). Equally, intra-clouds (vendor lock-in) migration generates relatively low concern rate (mean score = 3.70) among the users/potential users of cloud computing services, with some 40 (18.8%) of the respondents disagreeing with assertion that intra-clouds migration is a cause of concern in the cloud computing model.

Further, the data on concerns on cloud computing was tested using a Chi-squared test. The chi-squared test was used to determine whether there are significant concerns on cloud computing. This was done by using chi-square test whether the eight concerns raised by the top 100 SMEs organizations in Kenya are statistically significant. Response frequencies were grouped and summed in five levels, from strongly disagree to strongly agree, separately for the seven concerns raised. The data met the assumptions of independence and identical distribution of variables with none of the expected frequencies being less than 5. The Chi-square tests results are shown in Table 8.

Item	**n**	χ^2 value	Asymp. Sig.	df	**Conclusion**
Privacy	202	89.188	.000	4	Significant
Availability of services and/or data	202	46.515	.000	4	Significant
Integrity of services and/or data	202	4.287	.369	4	Not significant
Confidentiality of corporate data	202	48.347	.000	4	Significant
Loss of control of services and/or data	202	13.149	.011	4	Significant
Lack of liability of providers in case of security incidents	202	15.871	.003	4	Significant
Inconsistency between trans national laws and regulations	202	6.020	.198	4	Not Significant
Intra-clouds (vendor lock-in) migration	202	11.267	.024	4	Significant

Table 8:- Chi-Square Test Results on Concerns on Cloud Computing

The results in Table 8, shows that most of the concerns raised by the top 100 SMEs organizations in Kenya are statistically significant, $p< .05$, with those who agreed and strongly agreed that the concerns raised are serious forming majority of the respondents. Only two of the concerns did not meet statistical significance. For example, concern on integrity of services and/or data [$n= 202$; $\chi^2 (4) = 4.287$, $p=.369$] and inconsistency between trans national laws and regulations [$n= 202$; $\chi^2 (4) =6.020$, $p=.198$] were not significant.

IV. CONCLUSION

As a result of the findings in this research, the security challenges of Cloud Computing among selected SMEs in Kenya have been highlighted as stated in the objective. The major challenges highlighted in chapter four by the SMEs feedback can be summed up as follows.

- Data/information stored on the cloud may face a lot of availability issues due to downtime in the internet.
- A cloud administrator may become a very high risk if they turn rouge and try and access data stored on clouds.
- Because the owner of the data has not control over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way. His translates into loss of control over the data stored in the cloud.
- In SaaS model, hackers can manipulate weakness in data security model to get an illegitimate access to data or application.
- Multi-tenancy in the cloud a major issue for clients due to the possibility of a hacker taking advantage of the same host.

Similarly, as the findings suggest that Privacy, Availability of services and/or data, Integrity of services and/or data, Confidentiality of corporate data and Loss of control of services and/or data came out as the main concerns by the SMEs as they approach to Cloud Computing.

The bottom line for any SME is to achieve information security (confidentiality, integrity and availability) as is the case with all IT systems. Finally, policy makers and security designers can use this data on security challenges of cloud computing to make decisions on improving the overall security in the cloud.

REFERENCES

[1]. Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In *2011 World Congress on Information and Communication Technologies* (pp. 217-222). IEEE.
[2]. Centre for the Protection of National Infrastructure (CPNI). (2010). *Information Security Briefing*.
[3]. Creswell, J. W. (2014). *A concise introduction to mixed methods research*. Sage Publications.
[4]. Donald, K. K., & Delno, L. A. T. (2006). *Proposal and Thesis writing: An introduction*. Nairobi Kenya: Pauline Publications Africa.
[5]. Frankel, J. R., & Wallen, N. E. (2009). *Single-subject research: How to design and evaluate research in education*. (7th Ed.). New York, NY: McGraw-Hill.
[6]. George, E., Louw, D., & Badenhorst, G. (2008). Job satisfaction among urban secondary school teachers in Namibia. *South African Journal of Education*, *28*(2), 135-154.
[7]. Khajeh-Hosseini, A., Greenwood, D., Smith, J. W., & Sommerville, I. (2012). The cloud adoption toolkit: Supporting cloud adoption decisions in the enterprise. *Software: Practice and Experience*, *42*(4), 447-465.
[8]. Khan, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT Professional*, *12*(5), 20-27.
[9]. Kowalczyk, D. (2015). *Descriptive Research Design: Definition, Examples & Types*. Retrieved from https://study.com/academy/lesson/descriptive-research-design-definition-examples-types.html.
[10]. Nassiuma, D. K. (2000). Survey sampling. *Theory and methods.* Nairobi University Press.
[11]. Omwansa, K. T., Waema, M. T., & Omwenga, B. (2014). Cloud computing in Kenya. *Baseline survey*.
[12]. Oso, Y., & Onen, D. (2011). *Writing research proposal and report*. Nairobi: Jomo Kenyatta Foundation.
[13]. Padgett, D. K. (2016). *Qualitative methods in social work research* (Vol. 36). Sage Publications.
[14]. Palmer, S. A. (2015). *U.S. Patent No. 9,172,918*. Washington, DC: U.S. Patent and Trademark Office.
[15]. Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 693-702). IEEE.
[16]. Saripalli, P., & Walters, B. (2010, July). Quirc: A quantitative impact and risk assessment framework for cloud security. In *2010 IEEE 3rd International Conference on Cloud Computing* (pp. 280-288). IEEE.
[17]. Sen, J., & Sengupta, I. (2005, December). Autonomous agent based distributed fault-tolerant intrusion detection system. In *International Conference on Distributed Computing and Internet Technology* (pp. 125-131). Springer, Berlin, Heidelberg.
[18]. Shroff, G. (2010). *Enterprise cloud computing: Technology, architecture, applications*. Cambridge university press.
[19]. Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). *Computer security: Principles and practice* (pp. 978-0). Upper Saddle River (NJ: Pearson Education.
[20]. Zissis, D., & Lekkas, D. (2012). Is cloud computing finally beginning to mature? *International Journal of Cloud Computing and Services Science*, *1*(4), 172.