AN INVESTIGATION OF EMERGING RISKS ASSOCIATED WITH ONLINE BANKING ON FRAUDULENT PAYMENTS AMONG TIER ONE COMMERCIAL BANKS IN KENYA

[1]MAURINE AWUOR ONYANGO, [2]DR. COLLINS ODUOR ONDIEK

[1]Student from Department of Information Technology, Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya

[2]Lecturer School of Computing and Informatics, Universityof Nairobi, Nairobi, Kenya

E-mail: maurine266@gmail.com, ondiekcollins@gmail.com,

*Corresponding Author: Maurine AwuorOnyango: 0725246781

Abstract

Available statistics from across the worlddesignate that banking sector has suffered the highest fraudulent payment incidents andfirms losses no less than 5% of its yearlyreturns to fraud. This translates to approximately Kshs 13 Billion of the Kenyan's consolidated commercial banks returns in 2016. There is also evidence that fraudulent paymentrate is increasing in Africa as a whole and Kenya being on the top in Africa. Commercial banks in Kenya continued to adopt variety of technology, including online bankingduring the last ten years. It has however not been established whether the rise in fraudulent payments are as a result of online banking associated risks like operational risks, legal risks, and security risks. The study was set to find if online banking associated risks are related to fraudulent payments among within this sector. Study objectives were to: determine the effect of operational risks; establish the effect of security risks; and to establish the effect of legal risks on fraudulent payments. The study targeted 43 commercial banks licensed by Central Bank of Kenya from which 30 banks were sampled. Regression analysis was used to test the hypothesis that; no significant correlation between emerging risks in online banking and fraudulentpaymentsin commercial banks in Kenya. It revealed a positive and significant effect of emerging online banking on fraudulent payment among commercial banks in Kenya. The management of commercial banks are therefore provided with essential insights on the overall effect of emerging risks associated with online banking whichpresents a challenge to the regulatory authorities as to where their energiesought to be put in preventingbanking fraud in the sector.

Key Words**:** *Online BankingFraudulent Payment, Operational Risk, Legal Risk; Security Risk; Commercial Banks*

1.1 Introduction

The risk associated with fraud is immense, and the banking industry usesapproximately $67 billion per annum(Association of Certified Fraud Examiners, 2016). Globally, fraudulent payment is a major problem. The fraudulent payment occurrence is highest in the banking sector(Association of Certified Fraud Examiners, 2016). The firmstry to recover from worldwide financial headache and the world's major economies hang on the edge of downturn,fraudulent payment is a problem that cannot be ignored. What worries most is that this incidence is rising. For instance, the Survey in US by State of Cyber Crime revealed a yearly increase of 141 per cent in the number of financial institutions recording losses of between $10 million and $19.9 million in 2014. Its certain thatthis figure will be in the rise because many cases never get deliberatedabout with the external bodies for more investigations.

The global fraud study report shows thatfirm losses 5% of its annual revenue to fraud (ACFE, 2010)translating to approximately KShs 13 Billion as indicated by(CBK, 2011). The vice continues to threaten the expansion of businesses globally, ostensibly with the support of ICT such as online banking.It is not in doubt that emergence of Information and

Communication technology (ICT) has provided lots of opportunities aimed at organizations to improve on servicedelivery to its customers. Consequently, ICT helped in saving time, money and effort from an operational side. In reverse, cybercriminals are exploiting weaknesses in using ICT and working to develop sophisticated methods of computer crime attacks or introducing high-tech reinventions of old tricks (Waithaka, 2016).

Illegal entry into the information system of an organization during this era of ICT could have far reaching consequences. For instance, loss of privacy data could lead to lawsuits and litigations, and consequently loss of trust (Gaudin, 2007, cited in(Waithaka, 2016). Although internet and other forms of online banking is a blessing in the banking sector as far as speed, convenience, efficiency and cost of delivery, it has however been accompanied with various risks. In other words, ICT plays a double role as source of risks and a tool for work convenience. Because of rapid technological advances, there is no endin the types of risks or the control mechanismsaimed at those risks(Solanki, 2012), hence exposing organizations to variety of uncontrolled risks.

(Solanki, 2012)outlines three major categories of risks as: operational risks, legal risks, and security risks posed by the use of online banking, although studies linking the same to fraudulent payments among commercial banks in Kenya are limited. Operations risk arises from errors which occurs during processing, system interruptions, or other unexpectedhappeningsdue to an institution's inability to deliver products or services efficiently. According to(Barau, 2015), such risk include the risks relatedto communication breakdown, collapse of data processing, internal control system shortages, human faults and management failure. (Kiragu, Wanjau, Gekara, & Kanali, 2013)assert that operational risk is also caused by fraud. The financial institutionsexposed to operational risk from fraudcan experience financial loss from the parties involved. The banker's cheques are more vulnerable to loss or direct theft, whilein bank card payment transactionsfraud is the main concern.

Legal risk, on the other hand, is associated with of non-compliance with statutory or regulatory requirements that are related to electronic banking. (Okoro & Kigho, 2013)contend that legal risks comes from the uncertainty in the legal-regulative structure concerning online banking.(Hulme, 2011)argue that legal risk is linked with the protection of customers' personal information. Unauthorized persons canaccess banks databases and use customer's data to commit fraud(Kiragu, Wanjau, Gekara, & Kanali, 2013). In this case a legal risk is due to misuse of customers' data. Such risks are bound to increase due to uncertainty in thelawfulstructure and the specific legal regulations of transactions through internet.

Another type of risk associated with online banking is security risk. This is caused by unauthorized access to the customers' accounts and getting entree to the most importantdetails like accounting system, risk management system, portfolio management system(Solanki, 2012). According to(Barau, 2015), hackers get access, retrieve and use confidential customer information without their consent. They can also implant viruswhich cause loss of important customer's data, theft of important information,denial of service hence not being able to access bank's internal computer system thus. The banks will use a lot of money to repair those problems caused by viruses.(Waithaka, 2016). It was therefore essential to determine the existence of the aforementioned risks and relate them to fraudulent payments among commercial banks in Kenya.Violation of security leads to financial loss to the bank.

1.1.1Fraudulent Payment in Kenya

Theuniversalstanding of fraud as a risk in commercial banks is number 15 out of 25 risks identifiedit is however unique to East Africa. In East Africa fraud is ranked number 2 out of 25 risks inorder of perceived seriousness(PricewaterhouseCoopers, 2016). Compared to countries like Uganda, Tanzania, Rwanda and Zambia, the Kenyan banking sector has suffered most from fraud (PwC, 2016). The country experiences approximately 45% yearly increase in number of economic crimes associated with fraud(Government of Kenya, 2011). For instance, a staggering Kshs 1.7bn was lost by commercial banks in KenyafromAugust to October 2010 due to the vice. In addition, the sector lost Kshs 761Milion in the first six months of 2015due to fraud, as reported by Central Bank of Kenya(PricewaterhouseCoopers, 2016). The banking sector is very important for the Government of Kenya to help it in achieving itsvision 2030 dream. The things that needed to be improved arecoming up with asecure and dependable payments system to ensure smooth transfer of money between customers and banks as well as between the banks themselves. The use of mobile phone networks, internet and payment cards, operational resilience and security were to be looked at to ensure there is trust, integrity, availability and confidence in use oftechnologybased payment

systems(Government of Kenya, 2011). It is however unknown whether fraudulent claims experienced among Kenyan Commercial banks arose out of emerging risks associated with online banking.

1.2 Statement of the Problem

Commercial banks in Kenya are vulnerable to fraud than the other Eastern Africa countries. However these banks have constantlyimplemented risk management rulesgiven out by CBK for over five years. Kenya has the highest occurrences of fraud worldwide, almost doubling the global average of 34 % and significantly higher than the fraud incidence average in Africa of 57 per cent.In spite of the significant 84% (36) of commercial banks in Kenya conformingto risk managing guidelines issued by CBK, 95% of these banks aremore worried about fraud as a risk in banking transactions (CBK, 2016)due to losses the customers incur because of fraud. Escalating rate of fraud is really wearing down investor and consumer confidence which intimidates likely investors in Kenya (PwC, 2016). The research carried out by(Barau, 2015); (Kiragu, Wanjau, Gekara, & Kanali, 2013); (Okoro & Kigho, 2013) concentrated on the benefits of e-banking on performance of financial institutions without considering risks associated with online banking on fraudulent payments. It was therefore necessary to investigate the effect of emerging risks associated with online banking (operational risks, legal risks, and security risks) on fraudulent paymentsamongcommercial banks in Kenya. This study was set to bridge this gap.

1.3 Objectives of the Study

The main objective of the study was to find out effect of emerging risks in online banking on fraudulent payments in commercial banks in Kenya.

1.3.1 Specific Objectives

The specific objectives were to:

i. Determine effect of operational risks associated with online banking on fraudulent payments among commercial banks in Kenya
ii. Establish effect of legal risks associated with online banking on fraudulent payments among commercial banks in Kenya
iii. Establish effect of security risks associated with online banking on fraudulent payments among commercial banks in Kenya

1.4. Research Questions

The study sought to answer the following research questions

i. What is the effect of operational risks associated with online banking on fraudulent payments among commercial banks in Kenya?
ii. What is the effect of legal risks associated with online banking on fraudulent payments among commercial banks in Kenya?
iii. What is the effect of security risks associated with online banking on fraudulent payments among commercial banks in Kenya?

1.4.1 Hypothesis of the Study

i. There is no significant effect of operational risks associated with online banking on fraudulent payments among commercial banks in Kenya
ii. There is no significant effect of legal risks associated with online banking on fraudulent payments among commercial banks in Kenya
iii. There is no significant effect of security risks associated with online banking on fraudulent payments among commercial banks in Kenya

1.5 Scope of the Study

The research studyconcentrated on emerging risks associated with online banking among commercial banks. The emerging risks were categorised as operational risks, legal framework risks, and security risks. The study evaluated the

effect of the associated risks on fraudulent payments. Internal auditors, ICT managers, and financial accountants of 43 commercial banks operating in Kenyaparticipated in the study.

2.0 Literature Review

2.1Concept of fraud

Fraudulent payment isthe personal enrichment through payments made out falsified data or misrepresented information.An act of deliberate trickeryto secure something by taking discriminating advantage of another. It is dishonesty to gain while another's loss. **(S.P. Changalvaraya Naidu v. Jagannath, 1994)**

2.2 Theoretical Literature Review

The Fraud Triangle theory as advanced by (Albrecht, Albrecht, Albrecht, & Zimbelman, 2009) posits that three elements make up fraud: perceived pressure, perceived opportunity and rationalization of the act of fraud. Pressure relates to force caused by an employee's perceived abrupt urge to acquire assets, financial strains or fraud related issues(Albrecht, Turnbull, Zhang, & Skousen, 2010). Due to these pressures the fraudster take risks to obtain what they need. Fraudster must have a perceived opportunity to commit fraud or else they won't commit it. The perceived opportunities includes:not having strong board of directors, poor internal controls, hiding fraud behind complex transactions by those working in the banks or related-party structures. Opportunity is therefore a situation where a fraudster utilizes weakness in the system to make fraud possible (Rae & Subramaniam, 2008).Fraudsters always have a way tojustify their deeds as acceptable (Albrecht, Albrecht, Albrecht, & Zimbelman, 2009) not knowing that they are doing wrong to others.Lack of personal integrity or moral reasoning is often behind such acts (Rae & Subramaniam, 2008). This justification by fraudsters originates from the thinking that the sufferers owe them and that they arewarrantto more money (Mutua, 2011).

2.3 Empirical Literature Review

Online banking have been a good thing for banking sector. It improves on speed, convenience, efficiency and also reduces the cost of delivery. But it has come along with many threats and risks. It has also leadnew dimensions and new forms of risks (Solanki, 2012). Literature focusing emerging risks associated with online banking are however scant, particularly the ones involving commercial banks in the developing world including Kenya.

(Okoro & Kigho, 2013) provided a scrutiny on the challenges and viewsof e-transaction in the Nigeria. In the study the results showssignificant relationship between e-transaction andcountries economic growth.The problem is that it is still at its infant stage making it not possible to thrive in the right direction. The government, corporate bodies and individuals also have negative attitude towards e-transaction posing a big problem. These bodies havefears due insecurity, technical problems, anonymity, cultural problems which may be involved in such transactions.(Ngalyuka, 2013)investigated the relationship between use of ICT and fraud losses in commercial banks in Kenya and found that the total values transacted through EFT, RTGS and ATM had a positive correlation with the total fraud costs of commercial banks. It concluded that ICT utilization has exposed commercial banks in Kenya to more fraud.

The study by (Wekundah, 2015)on effects of cyber-crime on e-commerce for SMEs in Kenyapointed out that a big number of SMEs do not put more weight cybercrime attacks and they do not allocate enough resources on cybercrime attacks. It also revealed that they lack expertise and experiences in handling cybercrimes attacks.Another study by (Nyawanga, 2015)on the challenge of cybercrime on electronic transaction technologies in Kenyan banking sector, revealed that cyber-crime rate has increased in the last one year with 80% of cybercrimes mainly from China and Kenya. In most cases cyber-crime iscommitted by one of the bank staff when they know it or unknowing. Although the foregoing studies have dwelt on e-commerce and e-banking insecurities, they have not identified specific online associated risks such as operational risks, security risks, and legal risks.

3.0 Research Design and Methodology

3.1 Introduction

This section describes how data was collected, the population, sample size and sampling procedure, instruments for data collection, validity and reliability.

3.2 Research Design

This study employed descriptive and explanatory survey design. It was descriptive because data was collected through a detailed questionnaire which describes research questions, guided by hypotheses derived from adopted theories. Further, the study was explanatory since it sought to explain the relationship between emerging risks associated with online bankingand fraudulent payments. Descriptive and explanatory survey design entails collection of data by means of questionnaire, interviews, observations or telephone calls to discover opinions of a population based on a drawn sample size(Creswell, 2013); (Zikmund & Babin, 2010).

3.3 Target Population

Target population was all 43 Commercial banks operating in Kenya as at 30th June 2016 which are classified by the Central Bank of Kenya (CBK) using Market Share Index (MSI). 6 large banks operating in 546 branches, 15 medium banks operating in 310 branches and 22 small banks with 199 branches.

3.4 Sample Size and Sampling Procedure

Stratified method was used to get a sample size of 257 respondentsfrom 30 commercial banks. In addition, CBK annual reports were also used to determine the number of reported fraudulent payments during a period of 10 years (2006-2016). Among the sampled thirty commercial banks, increase in number of fraudulent payment (NFP) was determined by subtracting the number of fraudulent payments as at December 31, 2016 (nFP 2016) from the number of fraudulent payments as at December 31, 2006 (nFP2006). Log (Nfp.2016- nfp. 2006 was used to measure fraudulent payment.

3.5 Research Instruments

Questionnaire was used to collect primary data. Over 79% of the commercial banks in Kenya have centralized risk management model(Central Bank of Kenya, 2010)with the headquarters being in Nairobi. The research focused on head offices of each bank because branches generally mirror centralized risk management(Central Bank of Kenya, 2010).

3.6 Validity of the Instruments

Two independent professionals from the Certified Fraud Examiners, Kenya Chapter were contacted to assess content of the questionnaire to enhance validity. Likert-type scale of questionnaire ranging from 1 to 5 with the following equivalences, 1: ‘strongly disagree’; 2: ‘disagree'; 3: ‘neutral’; 4: ‘agree’; and: 5: ‘strongly agree'’ was used to measure the constructs. Likert scale is a suitable in determining attitudes and perception(Chimi & Russel, 2009).

3.7 Reliability of the Instruments

Reliability coefficient 0.97 was achieved using Cronbach alpha. The measure was considered adequate for the study(Cooper & Schindler, 2003).

4.0 Research Findings and Analysis

4.1 Questionnaire Response Rate

The questionnaire return rate was 89% (n=236) of which 25 (83%) of the banks had over 80% response rate.(Idowu, 2010)stated a response rate of 70% in their study on determinants of corporate crime in Nigeria which was a good

representation. Response distribution of the 236 respondents in terms of age was categorized between the age of 21 – 30 (28%), 31- 40 years (40%), 41-50 years (32%), over 50 years (2%). It means the respondents had sufficient knowledge on the subject of the study within the banking sector in Kenya. A significant 87% (n= 206) of the respondents had banking sector experience of between 1 and 10 years and were therefore likely to have required exposure to the subject of this study.

4.2 Relationship between Online Emerging Risks and Fraudulent payment

A descriptive analysis was carried out to establish the extent to which respondents consider reward system offered and ensuing fraudulent payment in the firm. Table 1 presents the results of the descriptive analysis of quantitative data.

Table 1: Descriptive analysis

	N	Minimum	Maximum	Mean	Std. Deviation
Fraudulent payment	236	1.00	5.00	2.1111	0.84096
Security risks	236	1.00	5.00	3.3300	1.25696
Operational risks	236	1.00	5.00	3.6970	1.12215
Legal risks	236	2.00	5.00	2.2068	.99725
Valid N (listwise)	236				

Source: survey (2018)

Table 1 indicate that respondents at Commercial banks consider fraudulent payment to have occurred only to a small extent (*M=2;* SD=0.84096). Similarly, legal risks was stated to be affecting fraudulent payment to a small extent (*M*=2.2068*; SD*=0.99725). However, the sampled respondentswere neutral (M=*3.33*; SD=*1.26*) with regard to whether security risksaffect fraudulent payment. Equally, the respondents agreed that operational security ((*M*=3.697; *SD*=1.122) affect fraudulent payment. It is therefore emerging from this finding that operational risks (*M*=3.697; *SD*=1.122) is the main component of emerging risks associated with online banking that tend to affect fraudulent payment in the company.

To determine the relationship between legal risks, operational risks, security risksand fraudulent payment in Commercial banks, the researcher used Pearson (r) correlation coefficients. Table 2 presents the results.

Table 2: Correlations between Online Emerging Risks variables and fraudulent payment

		Fraudulent payment	Legal Risks	Operational Risks	Security Risks
1	Fraudulent Payment	1			
2	Legal Risks	.-.164**	1		
3	Operational Risks	.816**	.224**	1	
4	Security Risks	.811**	.138**	.414**	1

**. Correlation is significant at the 0.01 level (2-tailed)

Source: Survey (2017)

Table 2 shows all the relationships between the dependent (fraudulent payment) and the independent (online banking associated risks) variables were significant ($p<0.05$). However, significant and positive relationships were found with two of the independent variables; operational risks (.816**, significant at the 0.01 level 2-tailed) and security risks (.811**, also significant at the 0.01 level 2-tailed). Similarly, significant but negative relationship was also found with legal risks (-.164**, significant at the 0.01 level 2-tailed). Equally, results in Table 2 show a significant relationship between operational risks and security risks (.414**, significant at the 0.01 level 2-tailed). This also implies that the more there are less of security risksamong commercial banks, the lower there will be operational risks and consequently lower fraudulent payments.

The researcher proceeded to conduct stepwise multiple regression analysis to examine effects of potential predictors (emerging risks associated with online banking) on fraudulent paymentamongCommercial banks. Table 3 presents results of the model of prediction using multiple regressions.

Table 3: Model of prediction using linear regression

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	1.218	.166		7.354	.000
	Legal Risks	-.428	.012	-.164	-4.179	.000
	Operational Risks	1.188	.093	.816	12.790	.000
	Security Risks	.601	.048	.811	12.414	.000

a. Dependent Variable: **Fraudulent Payment**

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.891[a]	.794	.792	.60088	.794	360.831	3	281	.000

a. Predictors: (Constant), Operational Risks; Legal Risks; Security Risks

Table 3 shows results from multiple regressions where the independent variables were legal risks, operational risks, security risks, while the dependent variable was fraudulent payment. It was established that these variables all together predicted about 79% of the observed variance in fraudulent payment, with a significant model fitting (F=360.83; p=0.000).

Findings from above revealed that the most important component of emerging risks associated with online banking in determining fraudulent payment was operational riskswith unstandardised beta (B=1.188; p<0.00). These results suggest that commercial banksare likely to displaylowerfraudulent payment if their operational risks levels are properly controlled. Itproves that security risks was significantly crucial in determining fraudulent payment (Beta=0.601; p<0.00). Therefore to improve on the fraudulent payment at Commercial banks, security risks for each employee need to be adequately controlled. Additionally, legal riskswith unstandardised beta (B= -.428; p<0.01) was found not to be significant in determining fraudulent paymentamong commercial banks.

5.0 Discussions, Conclusions and Recommendations

5.1 Discussions

Fraudulent payments among commercial banks are not easily detected since online banking are difficult to notice immediately as confirmed in Table 1 (M=2;SD=0.841), an indication that the respondents might not have been aware of fraudulent incidents. This tends to confirm what (Nyawanga, 2015)found out that cybercrime is difficult to detect in

timely manner since the attacks are perpetrated by one of the bank's staff knowingly or unknowingly. This also concurs with fraud triangle theory which highlights the circumstances in which an employee might be lured to commit fraud. (Waithaka, 2016) also established that cyber criminals are exploiting weaknesses in using ICT and working to develop sophisticated methods of computer crime attackshence corruption of data may lead internal employees to commit fraud unknowingly. The study also found out that there is significant relationship between emerging risks associated with online banking and fraudulent payments among commercial banks ($p<0.05$). This finding concurs with what (Solanki, 2012)established: that online banking has lead to new dimensions to risks and new forms of risks. This is despite the fact that online banking has been a blessing for banking as far as speed, convenience, efficiency and cost of delivery is concerned.

5.2 Conclusions

The study concludes that emerging risks associated with online banking: operational risks; security risks; and legal risks are significant determinants of fraudulent payments among commercial banks in Kenya. In most circumstances, the three variables contribute 74% of variance in fraudulent payment in commercial banks. This means that only 26% of variance in fraudulent payments in commercial banks is attributed to other factors other than operational risks, security risks, and legal risks.

5.3 Recommendations

In order for commercial banks to reduce fraudulent payments, there is needs to continuously improve on internal control measures that protect infiltration of information systems. Banks should adopt user identification measures through appropriate authentication methods; data identification and encryption; and cryptography technique should be used to secure the transmission of the data. Further research should be conducted on the challenges faced by commercial banks in adhering to legal frameworks asa measure in mitigating legal risks associated with online banking.

6. Acknowledgement
The author is most grateful to all managers of the commercial banks covered in the study. Their permission enabled data to be collected for the study. The author is also grateful to the Central Bank of Kenya for providing additional but critical data concerning banks and banking in Kenya.

REFERENCES

[1] ACFE. (2010). Report to the Nations on Occupational Fraud and Abuse,Global Fraud Survey.

[2] Albrecht, C., Turnbull, C., Zhang, Y., & Skousen, C. J. (2010). The relationship between South Korean Chaebols and fraud. Management Research Review, 33 (3), . 257-268.

[3] Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2009). *Fraud Examination. Natorp Boulevard, USA: Southwestern Cengage Learning.*

[4] Albrecht, W., C.C. Albrecht., C.O. Albrecht., & M.F. Zimbelman. (2009). Fraud Examination. South-Wester Cengage Learning, Mason, Ohio.

[5] Association of Certified Fraud Examiners. (2016). Report to the Nations on Occupational Fraud and Abuse, 2012 Global Fraud Survey.

[6] Barau, A. ,. (2015). Cyber Insecurity as a Manifestation of New Form of Global Urban Vulnerability. *at: https://www.researchgate.net/publication/283796419.*

[7] CBK. (2011). Central Bank of Kenya, Quarterly report on Development in theKenyan banking Sector for the period ended 30th June 2016. retrieved on 8th August 2016 www.centrabank.go.ke/downloads.

[8] CBK. (2016). Central Bank of Kenya, Quarterly report on Development in the Kenyan banking Sector for the period ended 30th June 2016. Retrieved on 8th August 2017 from http:www.centrabank.go.ke-downloads.

[9] Central Bank of Kenya. (2010). Bank Supervision report; Kenyan banking Sector for the period ended December 2010. Retrieved on 8th August 2011 www.centrabank.go.ke/downloads.

[10] Chimi, C., & Russel, D. L. (2009). "The Likert Scale. A proposal for Improvement Using Quasi- Continous Variables", Proc INSECON, 26, . pp. 1 -10.

[11] Cooper, D., & Schindler, P. (2003). Business Research Methods. (8th ed.). Boston: 15 McGraw-Hill Irwin.

[12] Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches. Sage.

[13] Government of Kenya. (2011). Kenya National Bureau of Statistics. Economic Survey 2011. Nairobi. Government Printer.

[14] Hulme, G. V. (2011). SCADA Insecurity-Stuxnet put the Spotlight on Critical Infrastructure Protection but Will Efforts to Improve it come too late? . *Information Security Magazine, 13(1),*, 38-44.

[15] Hussein, N., Khalid, A., & Khanfar, K. (2016). A Survey of Cryptography Cloud Storage Techniques. . *Int. Journal of Computer Science & Mobile Computing, 5 (2),* , 186-191.

[16] Idowu, A. (2010). An Assessment of Fraud and its Management in Nigeria Commercial banks. European Journal of Social Sciences, 10 (4), . 23 – 34.

[17] Kiragu, D. N., Wanjau, K. L., Gekara, M., & Kanali, C. ,. (2013). Effects of bank growth on banking fraud risks in commercial banks in Kenya. . *International Journal of Social Sciences and Entrepreneurship, 1 (3),*, 469-480.

[18] Mutua, F. (2011). Ksh.500m lost to Kenya bank fraud in just a month. National Health Care Anti- Fraud Association (http://www.nhcaa.org).

[19] Ngalyuka, C. (2013). The relationship between ICT utilization and fraud losses in commercial banks in Kenya. *Unpublished Project to University of Nairobi*.

[20] Nyawanga, J. O. (2015). Meeting the challenge of cyber threats in emerging electronic transaction technologies in in Kenyan banking sector . *(Doctoral dissertation, University of Nairobi).*

[21] Okoro, E., & Kigho, P. (2013). The problems and prospects of E-transaction: The Nigerian Perspective. . *Journal of Research in International Business and Management, 3(1)* , 10-16.

[22] PricewaterhouseCoopers. (2016). Spotlight on financial services 2011 Risk Survey www.pwc.com/ke/en/industries/banking.jhtml.

[23] PwC. (2016). Spotlight on financial services 2011 Risk Survey www.pwc.com/ke/en/industries/banking.jhtml.

[24] Rae, K., & Subramaniam, N. (2008). Quality of internal control procedures: Antecedents and moderating effect on organizational justice and employee fraud. . *Managerial Auditing Journal, 23 (2),* , 104-124.

[25] S.P. Changalvaraya Naidu v. Jagannath. (1994). Reported from Supreme Court of India. Reserve Bank Of India vs Bhopal Singh Panchal .

[26] Solanki, V. (2012). Risks in e-banking and their management. . *International Journal of Marketing, Financial Services & Management Research, 1 (9),*, 164 – 178.

[27] Waithaka. (2016). Factors affecting cyber security in national government ministries in Kenya. *Unpublished project submitted to University of Nairobi.*

[28] Wechuli, A. (2014). on Cyber Security Assessment Framework: Case of government Ministries in Kenya;. *International Journal of Technology in Computer Science and Engineering, 1(3).*

[29] Wekundah, R. N. (2015). The effects of cyber-crime on e-commerce; a model for SMEs in Kenya. *(Doctoral dissertation, University of Nairobi).*

[30] Zikmund, W., & Babin, B. (2010). Exploring marketing research. 10th Edition. USA:Thomson/South-Western.