International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 5 Issue 1, January 2018

ISSN: 2394-4404

A Framework For Secure Mobile Cloud Computing In Effective Electronic Learning

Laureen Akumu Ndeda

Solomon Ogara

Silvance Abeka

Department of Computer Science and Software Engineering,
Jaramogi Oginga Odinga University of Science and Technology, Kenya

Abstract: ***In the last few years, most universities have adopted E-Learning as a new approach to teaching and learning. However, the explosive growth and usage of mobile applications and the emergence of mobile cloud computing concept has raised questions about the reliability and privacy of devices in E-Learning. This paper investigates current challenges that affect the security of mobile cloud environment to E-Learning users, their network platform and data stored on the mobile devices with regard to issues of privacy, data ownership and concerns about device access and security. A total of 153 respondents from Kenyan universities participated in this survey. The results show that there is need to come up with a comprehensive secure solution for mobile cloud computing environment. This study is significant because it will help in research for a secure framework and enable organizations to secure their mobile cloud environment.***

Keywords: Mobile Cloud Computing, Security, Electronic Learning, Frameworks, Models, Standards.

I. INTRODUCTION

Kenyan universities are being compelled by the government within the framework of Kenya Vision 2030 to introduce e-learning and blended learning as an alternative delivery system to increase accessibility to higher education in Kenya (NESC, 2007). Mobile devices are being used today to perform most tasks that a desktop or laptop computer could be used for. On this premise, mobile devices are also used to connect to the resources of cloud computing hence, mobile cloud computing (MCC). The seemingly ubiquitous and pervasive nature of most mobile devices has made it acceptable and adequate to match the ubiquitous and pervasive nature of cloud computing. Mobile cloud computing is said to have increased the challenges known to cloud computing due to the security loop holes that most mobile devices have (Olayinka, Hani, & Silas, 2015).

A recent survey by Euro stats found out that four out of ten enterprises (Thirty Nine Percent) using the cloud reported the risk of a security breach as the main limiting factor in the use of cloud computing services while a similar proportion (Forty Two Percent) of those not using the cloud reported insufficient knowledge of cloud computing as the main factor that prevented them from using it (ENISA, 2010).

Mobile cloud computing technology is growing rapidly among the users and at the same time it introduces the new security threats. In recent years, hacking and malware applications have been targeting mobile devices and are found abundantly with applications downloaded in various categories such as entertainment, health, games, business, social 4 networking, travel and news. The popularity of these are easily available through mobile App-download centers such as Apple‘s iTunes, Nokia‘s Ovi suite and Android Google Play Store. This presents an added level of risk because essential services are often outsourced to a third party in Mobile Cloud, thus making it harder to maintain data security and privacy, support data and service availability, and

demonstrate compliance (Becher, Freiling, Hoffmann, Holz, Uellenbeck, & Wolf, 2011).

Mobile cloud computing is a new platform combining the mobile devices and cloud computing to create a new infrastructure, whereby cloud performs the heavy lifting of computing-intensive tasks and storing massive amounts of data (Satyanarayanan, 2010). In this new architecture, data processing and data storage happen outside of mobile devices. Gartner revealed that 2014 was the first year that majority of workloads were on the cloud as 51% was processed in the cloud versus 49% in the traditional IT space (Gartner Inc, 2012).

Universities and colleges in Kenya are already experiencing e-mail security challenges from the large student accounts that require dedicated servers and techies to guard against virus, worms, spam and other malware attacks," said Kevin Chege, a senior ICT officer at the Kenya Education Network (KENET), the ISP which brings together higher education institutions in the country (Sultan N, 2010).

It was estimated that by 2015, the mobile web will be bigger than desktop internet (Morgan S, 2010). This meant that majority of the entire world population will be using Smartphone's more than their computers. According to Dearbhla (2010), by the end of 2008, Kenya had more than 15 million mobile subscribers, with a mobile penetration rate of 39%. This shows a rise in Smartphone usage in Kenya therefore there is an emerging need to secure the device usage and its environment for better growth.

Mobile cloud computing brings a set of new challenges, especially when it comes to the availability of services and the security and privacy of consumers (Gu & Guirguis, 2014). Mobile devices such as cellular phone, personal digital assistant (PDA) and Smartphone's have also been exposed to numerous security threats like malicious codes (e.g., virus, worm, and Trojan horses) and thus pose as a vulnerability issue in the modern E-Learning environment. This has yielded various mobile security measures that address the various security gaps; however, the available measures that offer a comprehensive and secure mobile cloud solution to the E-Learning environment are inadequate thus influencing this research.

The purpose of this research is to investigate and develop a framework that can offer an adequate, comprehensive and a secure mobile cloud device environment. This study is therefore significant because higher learning institutions can use the framework for enhancing security in mobile cloud and policy formulation. This study can also benefit companies that have adopted or intend to embrace mobile cloud computing by providing them with a new perspective of looking at its security concerns. This way, the management of cloud service providers and its clients will be able to make sound decision based on the findings of this research alongside the existing security concerns.

II. LITERATURE REVIEW

A. MOBILE CLOUD COMPUTING IN E-LEARNING

As the Internet enabled devices including Smartphone's and tablets continue to grow, web-based malicious threats will continue to increase in number to make more complex. Securing data is now a more critical issue in the Mobile Cloud Environment. Cloud computing efficiently supports various tasks for data-warehousing, managing and synchronizing multiple documents online. Thus, mobile devices are no more constrained by storage capacity because their data is now stored on the cloud.

Mobile cloud computing is a new platform combining the mobile devices and cloud computing to create a new infrastructure, whereby cloud performs the heavy lifting of computing-intensive tasks and storing massive amounts of data (Satyanarayanan, 2010). Mobile users send service requests to the cloud through a web browser or desktop application. Then the management component of cloud allocates resources to the request to establish connection. Major data processing is migrated to 'cloud' thus the capability requirement of mobile devices is limited.

Learning resources are stored in clouds and are shared across different schools and universities. This equates to more educational resources availability for mobile cloud learning users. In addition, novel applications and services, which improve collaboration, can be implemented, such as collaboration tools between students of different institutions, social communities, and more (Hirsch & Ng, 2011). Mobile cloud learning can be easily accessed as long as a mobile network is available. Palmer and Dodson (2011) point out that rural student who do not have access to high-speed broadband Internet connections can access curriculum content easily via 3G mobile technologies. They can use services from the cloud data center for learning selected topics over their mobile phones even when they are in a small village or remote area (Rao, Sasidhar, & Kumar, 2010). Although one may need a subscription, mobile cloud learning is open access to everybody. The fact that people might access such a program through their mobile devices makes it convenient for them in any part of the world to access learning resources (Woodhill, 2010).

Mobile cloud learning is an amalgamation between cloud computing and mobile learning (Hirsch & Ng, 2011). It integrates the cloud computing into the mobile environment and overcomes obstacles related to mobile computing (Dinh, Lee, Niyato, & Wang, 2011). Mobile learning enables learners to acquire learning content anytime anywhere via portable devices. In mobile cloud learning, learners can access content, such as text-based documents, audio, and video files over the Cloud via their mobile devices connected with the Internet (Davcev & Kitanov, 2012). Mobile cloud learning is also flexible and allows for adjustments, depending upon learners needs. Since it is accessed through subscription, the user does not need to know where the learning sources are (Rittinghouse & Ransome, 2009).

B. SECURITY CHALLENGES

According to a survey (Subashini & Kavitha, 2011; Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009), 74% of IT Executives and Chief Information Officers are not willing to adopt cloud services due to the risks associated with security and privacy. To attract potential consumers, the cloud service provider has to target all the security issues to provide a completely secure environment.

Data/File Vulnerabilities: threats related to data security and confidentiality of the data. These attacks affect the data stored on the cloud. For owner the integrity of the data is very important. If any unauthorized person performs changes in data of other person then it can damage the integrity of the data (Khan et al, 2012).

Mobile Applications / Software Vulnerabilities: These mobile application models use the services of the cloud to increase the potential of a mobile device (Khan et al, 2012). Most users have Gmail, Face book, Whatsapp, Instagram, Drop box among others that normally collects data and operates in the phone's background. Unknowingly, the user may have downloaded the application from an unknown source and it could be spying and collecting information or even compromise the phone or its data.

User Vulnerabilities: A survey conducted by Sophos (2010) found that 26% percent of users' data was encrypted, 50% were not protected in the event of theft or loss of the device and 24% of users were not sure whether their Smart phone was encrypted. These results show that further education on the security dangers of Smart phones in mobile cloud is required. Mobile users often feel a concern about their data integrity on the cloud.

Network Vulnerabilities: As mobile users, there are several security threats like malicious codes like virus, worm, and Trojan horses that may emerge from the network. This is done by corrupting, blocking or modifying information on the wireless network by sniffing, spoofing or eavesdropping (Jeon, Jeeyeon, Youngsook, & Dongho, 2010).

Malwares: Malware can alter or expose private information in Smartphone's thus can risk mobile availability by meaningless operation (e.g. arbitrary code execution). Malware can also abuse costly services and functions like sending an SMS/MMS to unknown recipients or connecting to wireless networks without authorization (ENISA, 2010).

Denial of Service Attacks: An attacker can take advantage of an available Smartphone to make a denial of service attack to a base station, a wireless network or a web server. This can be done through usage of radio interference and cause denial of services of other devices on the network cloud (ENISA, 2010).

Code Breaks and Injections: An attacker can gain partial or full control over the target Smartphone on the cloud by using flaw of code, code injection or abuse of logic error to get information (ENISA, 2010).

Phishing: With mobile applications available on the touch/click on a mobile device and its convenience to the cloud, the user can expose his/her private information by accessing a phishing site e.g. through messenger phishing or through his/her private information by SMS phishing (ENISA, 2010). This can be done through an e-mail or SMS phishing to trick a user to access fake website to access business accounts.

Spam: This is whereby unsolicited messages and e-mails are received from known or unknown sources causing wastage of resources such as bandwidth and memory space (ENISA, 2010).

C. POLICIES, STANDARDS AND FRAMEWORKS

The table below summarizes the security Challenges for the frameworks available for cloud security:

Table 1: Security Frameworks and their Implementation Challenges in MCC (ISACA, 2011)

Framework Description	Challenges
ISO 27000/27001/27002 -Established by ISO. ISO2700x standards provide a security framework and process accreditation relative to the standards process.	-Few enterprises and education institutions are ISO 2700x-certified or understand the certification process. - Lack of guidance on implementation of the standards. - Not specifically focused on Mobile Cloud security. -No drill down into required specific actions during implementation and compliance with the standards. - Broad technical skills are needed for implementation. -Majorly needed when complying with federal laws and regulations. - Most companies using it majorly focus on market gains rather than on security.
NIST Framework for Security -Contains the controls required to address cloud security.	-Not specifically focused on unique cloud risk and standards especially on mobile cloud. -Does not provide independent, third-party assurance. - Not tried, Built and Tested on real security threats. - Not focused on financial or market gains. - Does not offer a worldwide certification as it dwells on guidelines for security. - Needs an in-depth understanding of security controls for implementation. - Difficult to implement in individual countries because of different set of laws and regulations. - Mainly suits large governmental organizations and limits usage in non-governmental organizations and small organizations.

ENISA Information Assurance Framework for Cloud Computing Defines multiple risk points in the cloud, covering the various delivery and deployment models. It is a detailed discussion regarding IT cloud risk.	- Not yet commonly understood or consistently accepted as a framework for cloud risk or mobile cloud security. -Limited to cloud risk and not focused on controls or tests of controls. -Does not provide independent, third-party assurance. - Needs technical skills for implementation. - Needs additional strategies for implementation.
Mobile Device Management (MDM) Framework -For full control of devices supported by API`s of Smartphone's to ensure device lockdown and policy enforcement.	- Not yet commonly understood or consistently adopted as a framework for mobile cloud risk. - Need Expertise and Technical experience when implementing. - Not widely recognized as a mobile security tool. - Does not differentiate between personal devices and company mobile devices.
Proposed Mobile Cloud Frameworks	-Most address only one or two parameters of security from the comprehensive set of authentication, integrity, confidentiality and privacy.

Table 1

D. LAWS AND REGULATIONS

The first policy for the cloud was issued in the US in 2010, mandating that all federal agencies give preference to cloud-based technologies over on-premises products. The federal risk and authorization management program (Fed RAMP) was created to support this plan and standardize agencies' security requirements.

The congress enacted the Health insurance portability and accountability act (HIPAA) partly to standardize the security and privacy requirements of healthcare-related data systems. Compliance with HIPAA is mandatory for healthcare organizations, meaning it's also a non-negotiable for cloud providers looking to attract them (Narcisi, 2012).

Large American providers of cloud services, like Amazon, Google, Azure among others have data centers throughout Europe. These European companies with American subsidiaries are vulnerable to American law enforcement requests, a point of contention between the other global governments like Kenya which have their own laws.

The telecommunications market in Kenya was broadly liberalized in 1999, giving more scope for private sector innovation and market entry. The Communications Commission of Kenya (CCK) was established to regulate the sector and, for the first time, issued ISPs with licenses. However, the former incumbent Telco (now renamed Telkom Kenya) retained a monopoly to operate the Internet gateway and backbone until mid-2004. During this period, it expanded the national backbone, but available international bandwidth did not increase rapidly until after the end of Telkom's exclusivity period. Shortly after this ended, CCK licensed two additional Internet Backbone Gateway Operators, and allowed telecommunications businesses – including Telkom and the mobile operators Safaricom and Celtel – to offer mobile Internet services in competition with stand-alone ISPs (CAK, 2008).

CCK commissioned a market study of the Internet in Kenya in 2006/7. This suggested that some 2.7 million Kenyans were then using the Internet, 80% of them in Nairobi, and that the market was constrained by high costs, poor regulatory governance (for example in spectrum management) and the lack of locally relevant content. Its recommendations envisaged the development of a market of 8 million users, to be encouraged by government and regulatory interventions including improved national fiber infrastructure (CAK, 2008).

While the increasing availability of the Internet through mobile devices has greatly increased individual access over the last two years or so, many Internet users in Kenya rely on access in workplaces, educational institutions and cybercafés. Government agencies, and multi-stakeholder or public/private partnerships coordinated by government agencies, play a significant part in technical governance of the Internet in Kenya. CCK, the ICT Board and the Directorate of e-government all play a part in other governance bodies with Kenic in charge of .ke Domains.

E. INFORMATION SECURITY ATTRIBUTES AND GOALS

SysAdmin, Audit, Network, Security (SANS) defines information security as processes and methodologies which are intended to protect sensitive information or data from unauthorized access, disclosure, modification, or use. The form of the protected data or information can be electronic, printed, or other forms (SANS, 2010). Information security encompasses major fundamental security attributes/goals namely confidentiality, integrity, availability, Authentication and NonRepudiation. The presence of these attributes characterizes well secured information (Allen, Barnum, & Ellison, 2008).

F. CONCEPTUAL FRAMEWORK

The conceptual framework included the independent variables being the type of smart devices, Data stored by the respondents, security controls and measures available at the institution, type of security threats and attacks that affect mobile cloud environment, the effects of the attacks and lastly the available security models. The dependent variables were the security goals of confidentiality, integrity, availability, authentication and non-repudiation. The intervening variables included laws, service level agreements, guidelines and procedures for mobile cloud security.

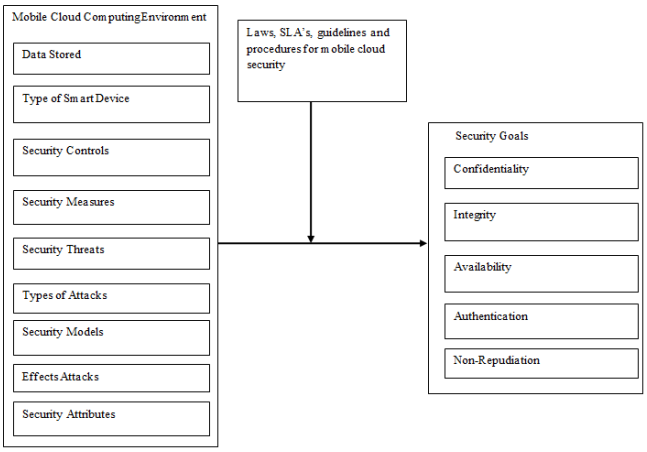

Figure 1: Conceptual Model

III. RESEARCH METHODOLOGY

This study utilized a cross-sectional descriptive survey with quantitave methods as it was useful at investigating and providing an in-depth insight into Mobile Cloud Computing security in E-learning in public institutions of higher learning (Fraenkel, Wallen, & Hyun, 2012). The population of the study was the staff and students who use Mobile Cloud in eight major universities offering E-Learning, four public and four private universities in Kenya.

The study was conducted in eight major universities in Kenya. These universities offer electronic learning as a form of education for award of degrees and the target population access E-Learning materials through mobile devices and Smart phones. The study utilized a cross-sectional descriptive survey with quantitave methods as it was useful at investigating and providing an in-depth insight into Mobile Cloud Computing security in E-learning in public institutions of higher learning (Fraenkel, Wallen, & Hyun, 2012).

The population of the study consisted of employees and students who use Mobile Cloud in E-Learning among the selected universities in Kenya The selection of the these universities was informed by the fact that they are the extreme opposite of each other in terms of years of operations, size, profitability and workforce. This ensured that the study cut across the big and already established players in the Academic sector in Kenya. Sample size was selected based on Yamane formula (Yamane, 1967) with the outcome displayed in table 2 below:

Name of the University	Target Population of MCC Users in E-Learning	Selected Sample size using Yamane's Formula	Sample Size	
			Number of staff	Number of students
University 1	50 Users.	45	8	24
			Total number of sample size = 32	
University 2	30 Users	28	7	19
			Total number of sample size = 26	
University 3	30 Users	28	5	19
			Total number of sample size = 24	
University 4	30 Users	28	5	20
			Total number of sample size = 25	
University 5	10 Users	9	2	8
			Total number of sample size = 10	
University 6	10 Users	9	2	6
			Total number of sample size = 8	
University 7	15 Users	14	2	7
			Total number of sample size = 9	
University 8	20 Users	19	3	16
			Total number of sample size = 19	
Total Number	195 Users	180 Users	153 Users	

Table 2: Sample Size Determination

This research project employed the use of self administered close-ended structured questionnaire. This was guided by the vast nature of the data that was to be collected, the time available and the objectives of the study.

Data collection instrument was pretested to determine their validity and reliability. The questions were formulated by the researcher and tested to ensure their conformity. Face Validity and Content Validity approach was used for the study. In content validity, the data instrument was tested in a pilot study to establish if it contains all possible items that was to be used in measuring the concepts (Rugg & Petre, 2007). This confirmed that there were enough items and questions in instrument covering the study topic. The researcher used the expert judgment method to determine Face validity. A copy of the questionnaire was given to the supervisor to check if it represented all the objectives of the study.

Test-retest reliability was used for this study (Sekaran & Bougie, 2010). The test-retest was administered to staff and students of the universities and the same test was also administered after 2 weeks. The scores from time 1 and time 2 were then correlated in order to evaluate the test for stability of time. To measure the degree to which the questionnaires will yield consistent result or data, the researcher computed the Cronbach's coefficient Alpha technique to establish how items correlate amongst themselves to determine reliability. Evaluation of the framework was done using correlation and regression analyses and this confirmed the suggested relationships between variables in the framework.

Reliability Statistics	
Cronbach's Alpha	N of Items
.843	37

Table 3: Cronbach's alpha reliability test value

This meant all constructs were internally consistent and measured the same content of the construct. The findings thus show that the questionnaire used in the study was reliable and the results of the questionnaire can be relied on as the alpha values were above 0.70.

IV. RESULTS

Responses from the questionnaires were summarized, edited, coded and allocated frequencies following the likert scale responses ratings to establish the mean, mode, variance, standard deviation and the correlation between variables. The descriptive statistical method analysis was applied to measure and determine the relationship that exists among the collected data. Demographics was analyzed using frequency graphs and the objectives analyzed using mean and standard deviation. The data was then analyzed descriptively with the mean and mode usage to understand and interpret variables. These allowed the analysis and presentation of large amount of data to be collected in the field. The researcher used SPSS Software program to analyze the data and present it in form of pie charts, graphs, and tables among others. The data analysis was carried out after the data entry of all the questions was complete. Descriptive statistics formed the basis for presenting the data collected. Frequency and percentage distributions indicating the number of occurrences of each category were used to reveal the patterns and thus to facilitate interpretation. The descriptive statistics were generated using SPSS 20 for windows.

The study used regression model to determine the relationship between the dependant and the independent variables. The Pearson product moment coefficient (R) was used to establish the association between the independent and dependent variables based on the population data. A co-efficient of determination (R2) was performed to determine how much of the dependent variable comes about as a result of the independent variable being tested. The study tested R2 at 95% significance level. To test the significance of the findings, analysis of variance (ANOVA) was done to determine if the independent variables have an effect on each of the dependent variable.

The study found out that 14.4% were diploma holders and majorities were between the ages of 18-24. The study found out that 67.3% represented the number of degree holders with majority of the respondents within the age bracket of 18-24, 25-30, 31-34 and lastly over 35 respectively. The study however showed a shift with Masters student's who represented 17.7% of the total respondents and their age gap ranged from 25years to Over 35 years. The percentage represented by PHD respondents was 0.6% and the age group was over 35 years. The study also showed students as the major respondents at 72% and majority belonging to the 18-24 age group while Staff represented 28% with Majority belonging to 25-30 age group. Lastly, all the respondents admitted to having mobile devices.

		Age of respondents					
		18-24	25-30	31-34	over 35		Totals
		Count	Count	Count	Count	Percentages	
Education level of respondents	Diploma	12	4	4	2	14.4%	
	Degree	65	30	6	2	67.3	
	Masters	0	10	10	7	17.7	
	PHD	0	0	0	1	0.6%	100%
Position at the University	Staff	2	20	11	10	28%	
	Student	75	24	9	2	72%	100%
Do you have a Mobile Device used to access the Internet at your University?	Yes	77	44	20	12	100%	
	No	0	0	0	0	0%	100%

Table 4: Bio-data of the respondents

The study also found that 98.7% of users used smart phones to access academic materials in E-learning compared to 1.3 % who do not use Smartphone's in accessing E-Learning materials, 92.8% also said they use laptops as compared to 7.2% who don't use Laptops in E-learning. With the use of Ipad, 13.1% percent said they use Ipad to access E-Learning whilst 86.9% said they don't use Ipads. In conclusion, 42.5% used tablets in E-Learning whilst 57.5% said they don't use tablets.

The study also sought to find out the respondents type of applications stored on their mobile devices that they use in E-learning. From the above chart, the researcher found out that Majority of the staff at the Universities store Mobile Apps, Emails, Administrative Documents, Class Notes, Business Applications, Class Assignments, Student Exams and Passwords at 100%, 93%, 93%, 86%, 72.1%, 55.8%, 48.8% and 39.5% Respectively While Passwords, Students Exams, Class Assignments, Business Applications were not majorly Stored by most of the Staff respondents on their Mobile Devices.

For the Students, data stored on the devices were mobile applications, class notes, emails, class assignments, passwords, business applications and administrative documents at 100%, 99.1%, 90%, 85.5%, 43.6%, 25.5%, and 2.7% respectively. There was no record found on storing student exams on the student's Mobile Devices.

Additionally this study sought to find out whether they have encountered any security challenges when accessing E-Learning materials on the cloud using their mobile devices. The answers are portrayed below:

Security Challenges Acceptance / Denial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	148	96.7	96.7	96.7
	Not Sure	5	3.3	3.3	100.0
	Total	153	100.0	100.0	

Table 5: User experience on security threats and attacks

From the above table, 96.7% said that they have experienced security threats and attacks while 3.3% said they were not sure. None of the participants denied ever experiencing security attacks on the mobile cloud.

TYPES OF SECURITY CHALLENGES EXPERIENCED WITH MOBILE CLOUD

The researcher set to find out the type of security challenges that affects the respondents when using mobile devices in the cloud in E-Learning. The percentage of respondents who have experienced Data/File Loss, Virus Attacks, Phishing, Phone Freeze, Corrupted Documents, Slow Data Loads, Email Spams, Malwares and Insecure Internet was 28.8%, 78.4%, 19%, 68%, 79.1%,67.3%, 63.4%,54.9% and 37.3% respectively. The percentage of those who said no

to the above incidences was 71.2%, 21.6%, 81%, 32%, 20.9%, 32.7%, 36.6%, 45.1% and 62.7%. Majority of the respondents said that they experienced Virus attacks, Corrupted Documents, Phone Freeze/Hangs, Slow data Loading, Email Spams, Malwares, Insecure Network and Data/File Loss respectively in Descending Order from Highly experienced attack to the lowest experienced attack respectively.

EFFECTS OF THE SECURITY CHALLENGES

The researcher also set to find out the effects of the security challenges from the respondents when using mobile devices in the cloud in E-Learning. 37.3% of the respondents reported of having experienced an insecure network due to an attack while 62.7% of the respondents have not experienced that. 34% of respondents reported of having internet/Network Interruption due to security attacks in Mobile Cloud while 66% did not. Also, 16.3% of respondents said their mobile devices were destroyed due to attacks in mobile cloud as compared to 83.7% who did not experience that effect. Also, 61.4% of respondents said their academic materials on Mobile Cloud were destroyed as compared to 38.6% whose materials were not destroyed due to security attacks. 19.6% of Users reported that their identity was compromised due to security attacks while 80.4% of respondents have not experienced that. Also, 19% of respondents reported that their mobile devices were compromised in opposite of 81% of respondents whose devices were intact and lastly, 60.1% of respondents said that their data was deleted following attacks on Mobile Cloud while 39.9% of respondents data were not deleted.

SECURITY THREATS IN INSTITUTIONS

The researcher sought to find out whether the respondents have experienced the following Security Threats and Risks in the University E-learning platform. None of the users strongly disagreed on experiencing data loss while 46.4% disagreed, 2.6% were undecided, 48.4% agreed and 2.6% strongly agreed on experiencing data loss. On Virus threats, 13.1% disagreed on ever experiencing virus threats while 81.7% agreed and 5.2% strongly agreed. None of the users strongly agreed or were undecided on ever experiencing virus threats. Malware threats saw 3.9% disagreeing on ever experiencing malwares, while 41.2% were undecided.48.7% agreed and 5.2% strongly agreed to having experienced the malware threat. When it came to Phishing attacks, 68.6%, 5.2% 24.8% and 1.3% disagreed, were undecided, agreed and strongly agreed respectively. Users who have answered on phone freeze attacks were 45.1%, 2.6%, 51% and 1.3% on Disagree, Undecided, agreed and strongly agreed respectively. On Email Spams, 17.6% Disagreed, 4.6% were undecided, 76.5% agreed and 1.3% strongly agreed on their experience with Email Spams. When it came to attacks that corrupt documents, 8.5% disagreed on ever experiencing such kind of attack while 3.35 were undecided, 60.8% agreed and 27.55 strongly agreed on the attack experience. Also, 21.6% disagreed on ever experiencing attacks that led to slow data loading, 3.3% were undecided, 64.1% agreed and 11.1% strongly agreed to having the attacks that led to slow data loading. With regards to attacks that led to insecure internet/Network, 71.9% disagreed on ever experiencing such attacks while 4.6% were undecided, 20.9% agreed on experiencing the attack and 2.65 strongly agreed to experiencing such attacks. Lastly, with regards to the lack of security guidelines at the institutions, 6.5% were undecided, 68.6% agreed and 24.8% strongly agreed that there was lack of security guidelines at their institutions.

SECURITY MEASURES IN INSTITUTIONS

The researcher also sought to find out whether the respondents have knowledge of the following Security Measures on the University E-Learning Platform. From the findings, 0.7% were undecided as to whether they have E-Learning Passwords and Logs, 855 agreed and 14.45 strongly agreed to having the passwords. None of the users strongly disagreed or disagreed with the statement. Also, 24.2% Disagreed on having Antivirus as a security measure while 32.7% and 43.1% were undecided and agreed respectively. None of the users strongly disagreed or strongly agreed to having an antivirus as a security measure. 76.5% disagreed to having firewalls as a security measure, 13.1% were undecided and 10.5% agreed to having firewalls. With the use of Secure Logging, 73.2% disagreed on having secure logs while 20.9% and 5.9% were undecided and agreed respectively. 88.9% of users disagreed on the availability of security policy documents as a security measure while 4.6% and 7.2% were undecided and agreed respectively. None of the users strongly disagreed or strongly agreed with the statements.

SECURITY CONTROLS IN INSTITUTIONS

The study sought to find out whether the respondents have knowledge of the following Security Controls at their institutions. From the above chart, 0.7% were undecided as to whether they have E-Learning Passwords and Logs, 85.5% agreed and 14.45% strongly agreed to having the passwords. None of the users strongly disagreed or disagreed with the statement. Also, 24.2% Disagreed on having Antivirus as a security measure while 32.7% and 43.1% were undecided and agreed respectively. None of the users strongly disagreed or strongly agreed to having an antivirus as a security measure. 76.5% disagreed to having firewalls as a security measure, 13.1% were undecided and 10.5% agreed to having firewalls. With the use of Secure Logging, 73.2% disagreed on having secure logs while 20.9% and 5.9% were undecided and agreed respectively. 88.9% of users disagreed on the availability of security policy documents as a security measure while 4.6% and 7.2% were undecided and agreed respectively. None of the users strongly disagreed or strongly agreed with the statements.

EXISTING SECURITY MODELS, STANDARDS AND FRAMEWORKS

The study sought to find out whether the respondents have knowledge of the following security models, standards and frameworks. From the findings, majority of the respondents said that they were not aware of the currents standards, models and frameworks of NIST, MDM, ISO 27001/27002, ENISA, CLOUD Control Matrix, Mobile

Policies and Mobile Devices Controls. We however see a shift of answers whereby majority of the respondents knew about an existing ICT policy at the institutions.

SECURITY ATTRIBUTES

The study sought to find out whether the respondents have knowledge of the major security attributes. From the findings, Majority of the respondents only knew of authentication / authorization but on the other hand, majority of the respondents had little or no knowledge security goals of confidentiality, integrity, availability and non-repudiation. Correlation analysis was performed on the variables and the results shown below. A Pearson's correlation coefficient was computed to assess the relationship between the independent variables and dependent variable as summarized in Table 4. The correlation results in the table enabled the researcher to assess the relationship between the variables under study.

	Smart Device	Data Stored	Type of Attack	Attack Effects	Sec Threats	Sec Measure	Sec Model	Sec Attributes	C	I	A	A	N
Smart Devices	1												
Data Stored	.225**	1											
Type Of Attacks	0.039	-0.002	1										
Attack Effects	0.004	-0.049	0.046	1									
Sec Threat	0.017	0.057	0.079	0.061	1								
Sec Measures	-0.152	-0.068	0.049	0.056	.372**	1							
Sec Models	-0.073	-0.07	0.057	0.073	.179*	.460**	1						
Sec Attributes	0.043	0.137	-0.133	0.069	-0.135	0.035	0.13	1					
C	0.07	.222**	0.087	0.074	-0.059	0.09	-0.12	.822**	1				
I	0.016	0.038	0.101	0.087	0.142	.218**	-0.006	.708**	.492**	1			
A	0.02	.159*	-0.078	-0.048	335**	-0.005	-.174*	.569**	.359**	0.047	1		
A	0.034	0.059	-0.096	0.077	-0.136	-0.024	-0.149	.827**	.542**	.518**	.348**	1	
N	-0.065	0.043	.186*	0.037	.219**	0.052	.240**	.348**	.180*	.176*	0.12	.360**	1

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Table 6: Correlation analysis

Coefficient of determination (the percentage vasnippriation in the dependent variable being explained by the changes in the independent variables) and P-value were used to determine the overall significance of the model. Multiple regression analysis was conducted to test the overall effect of all the independent variables on the each dependent variable. Analysis of variance (ANOVA) was used to test the hypothesis of the multiple regression model shown below:

y (dependent variable) =β^0 + $\beta^1 x1$+ $\beta^2 x2$+ $\beta^3 x3$+ $\beta^4 x4$+$\beta^5 x5$+ $\beta^6 x6$+ $\beta^7 x7$+$\beta^8 x8$+e

Where; x^1= Smart Devices, x^2= Data Stored, x^3= Type of Attacks, x^4= Attack Effects, x^5= Sec Threats, x^6= Sec Measures, x^7= Sec Models, x^8= Sec Attributes and e=Error

β^0, β^1, β^2, β^3, β^4, β^5, β^6, β^7 *and* β^8 are model parameters and they describe the directions and strengths of the relationship between the dependent and the independent variables. β^0 is a constant (intercept).

CONFIDENTIALITY

The researcher conducted a multiple regression analysis so as to determine the relationship between the Security goal of Confidentiality and all the other Variables.

Confidentiality = 2.089 + 0.024 Smart Devices + 0.028 Data Stored+ 0.054 Attack Effects+ 0.020 Type of Attacks + 0.044 Sec Threats+0.078 Sec Measures + 0.307 Sec Controls+0.013 Sec Models + 0.099 Sec Attributes + ε

INTEGRITY

The researcher conducted a multiple regression analysis so as to determine the relationship between the Security goal of Integrity and all the other Variables.

Integrity = 2.456 + 0.302 Smart Devices+0.056 Data Stored+ 0.041 Attack Effects+ 0.115 Type of Attacks + 0.406 Sec Threats + 0.307 Sec Measures + 0.359 Sec Controls + 0.225 Sec Models + 0.969 Sec Attributes + e

AVAILABILITY

The researcher conducted a multiple regression analysis so as to determine the relationship between the Security goal of Availability and all the other variables.

Availability= 3.479 + 0.009 Smart Devices + 0.034 Data Stored + 0.186 Attack Effects + 0.042 Type of Attacks - 0.408 Sec Threats + 0.389 Sec Measures – 0.416 Sec Controls - 0.247 Sec Models+ 0.735 Sec Attributes + e

AUTHENTICATION

The researcher conducted a multiple regression analysis so as to determine the relationship between the security goal of Authentication and all the other variables.

Authentication = 2.159 + 0.151 Smart Devices + 0.057 Data Stored + 0.089 Attack Effects + 0.109 Type of Attacks + 0.086 Sec Threats + 0.079 Sec Measures + 0.124 Sec Controls +0.135 Sec Models + 0.275 Sec Attributes+ ε

NONREPUDIATION

The researcher conducted a multiple regression analysis so as to determine the relationship between the Security goal of NonRepudiation and all the other variables. Results portrayed a positive and statistically significant relationships in all the variables shown by p=<0.05. This implies that all variables are some of the major Influences in ensuring NonRepudiation in Mobile Cloud Security.

NonRepudiation = 1.978 + 0.049 Smart Devices +0.102 Data Stored + 0.014 Type Of Attacks + 0.010 Attack Effects+0.047 Sec Threats+0.044 Sec Measures+0.019 Sec Controls+0.001 Sec Models + 0.250 Sec Attributes + ε

The study found that there is a very strong correlation between the variables Attack Effects, Type of attacks, Sec_Threats, Sec_Measures, Sec_Controls, Sec_Models And Sec_Attributes thus affecting heavily on the security of mobile cloud. On the other hand, type of smart devices and data stored also have a little but significant effect on mobile cloud computing security.

VALIDATED FRAMEWORK FOR MOBILE CLOUD COMPUTING

The result of this study is a secure framework for mobile cloud which included all the variables in the conceptual framework tested using regression analysis to identify if they have a significant impact on the security of mobile cloud. The validated framework (Figure 3 below) emphasizes on the

ISSN: 2394-4404

utilization of user involvement in order to determine the organizational goals and objectives.

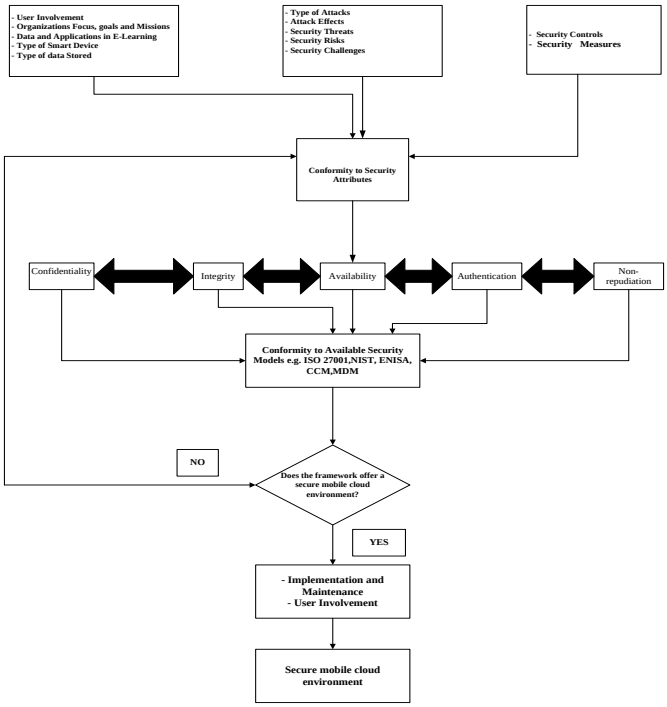

Figure 3: Framework for mobile cloud security

V. DISCUSSION

From the findings, 96.2% said that they have experienced security threats and attacks while 3.8% said they were not sure. None of the participants denied ever experiencing security attacks on the mobile cloud. The attacks experienced include data/file loss, virus attacks, phishing attacks, phone freeze, corrupted document, slow data loading, email spams, malwares and insecure internet/network. The study found out that virus attacks, corrupted documents, slow data loading, phone freeze, email spams and malwares are the leading attacks experienced while data loss and insecure network are the least experienced attacks.

The study also found out that majority of the institutions allowed the respondents to use their mobile devices and when it comes to mobile cloud usage guidelines, 62.7% which represented majority of the respondents, said that they do not have mobile cloud device usage at their institutions while 22.7% of the respondents were not aware on the guidelines and 15.2% of respondents agreed that there was guidelines on mobile cloud usage at the institutions. This findings portrayed that majority of the institutions do not have mobile cloud usage guidelines.

About security threats experience by respondents on the E-Learning platform at the institutions, the study found out that the highest number of threats were the major lack of security guidelines, viruses, threats that corrupt data, email spams, threats that cause slow data loading, malwares and threats that cause phone freeze while the lowest category of threats experienced by respondents include threats that leads to data loss, phishing and threats that cause a network to be insecure.

The researcher also sought to find out the existing security measures and controls available at the institutions. From the findings, login passwords and to a lesser extent, antivirus software was found at the institutions. However a larger number of respondents reported that there were no firewalls, secure logging, security policies and mobile policies at the institutions. Concerning the security controls available at the institutions, majority of the respondents said agreed that their institutions have physical controls like control circuits TV and alarms and technical controls like encryption, smartcards e.t.c in their various institutions. However, majority of the respondents disagreed and reported that they don't have administrative controls like training and awareness on mobile cloud security, disaster preparedness and recovery plans e.t.c.

The study sought to find out whether the respondents have knowledge of the following security models, standards and frameworks and the findings were that majority of the respondents had little or no knowledge of NIST framework, Mobile Device Management framework, ISO standards, ENISA framework, Cloud Control Matrix framework, Mobile Cloud Controls and their policies. Also, majority of the respondents knew mostly about an ICT policy.

The study also sought to find out user experience with the five major security attributes at the institutions and whether they are effective at the institutions. From the findings, Availability, Integrity and Accountability were highly maintained at the various institutions respectively, followed by Confidentiality and lastly Non-repudiation attribute. The study therefore found out that there is still need to implement the above security attributes at a higher level in mobile cloud computing usage in institutions and Kenya as a whole.

After performing regression analysis, an increase in the independent variables impacted towards an increase in each of the dependent variables. The study found that there is a very strong correlation between the variables ATTACK EFFECTS, TYPE OFATTACKS, SEC_THREATS, SEC_MEASURES, SEC_CONTROLS, SEC_MODELS and SEC_ATTRIBUTES thus affecting heavily on the security of mobile cloud. On the other hand, types of Smart devices and Data Stored also have a little but significant effect on mobile cloud computing security.

VI. CONCLUSION

The survey revealed that 95% of the Institutions allowed the use of mobile devices for cloud and work related tasks. The devices allowed included Smartphone's, laptops, iPads and tablets. However, we see security related challenges and threats like viruses, malwares, phishing attacks, attacks leading to data loss and data corruption, email spams among others. The study also found out that the above security challenges led to internet / network interruption, destruction of mobile device, destruction of academic materials in E-learning, user compromise, mobile device compromise and deletion of data files and folders.

On security measures and controls implementation at the institutions, majority of the respondents reported of passwords and logs with antivirus software in the institutions. We see

other major security measures missing. About security controls, majority of the respondents reported physical and technical security controls; the gap on administrative controls is clearly seen.

On user knowledge of security frameworks, standards and models in mobile cloud usage, majority of the respondents are not aware of the major frameworks like NIST, ISO 27001/27002, Mobile Device Management framework, ENISA framework, Cloud Control Matrix framework, Mobile Cloud Controls and their policies. The study found out that majority of the respondents knew mostly about an ICT Policy. This revealed a gap in user knowledge and trainings on frameworks. About user knowledge and experience with security attributes, availability, integrity and accountability was highly maintained while confidentiality and Non-repudiation security attributes were least implemented. When performing regression analysis, the study was found to be significant. In correlation analysis, the variables revealed relations amongst them.

VII. RECOMMENDATION

Organizations therefore should take an awareness and sensitization approach. From the study, the attacks are happening and the effects are trickling in. Security controls and more measures should be put in place. There is also an equal need for implementation of a framework that is suitable for mobile cloud usage and encompasses all user needs. The security policies should be reviewed to ensure they also cater for and include mobile cloud usage control and management. Training and awareness programs should be developed to enlighten all stakeholders. Lastly, like other information technology security frameworks widely known, there are issues other than the Mobile Cloud technology that need to be taken into account for example compatibility of the framework with organizational policies, structures, Goals, values, legal frameworks and most importantly, organizations will have to assess the necessity of Mobile Cloud usage implementation, its usefulness in security and the framework compatibility with major security goals.

Further research includes the need to look for widely known and worldwide recognized frameworks. Majority of mobile cloud businesses are using the cloud to create business advantage. Further research also needs to identify the issues faced by organizations when adopting the cloud. Since mobile cloud computing is still new to both academia and commerce the outcome of these studies will help academics and practitioners alike assess the actual uses of the cloud in practice and the business benefits and challenges of adopting it.

REFERENCES

[1] Allen, J.H, Barnum, S., & Ellison, R.J., McGraw, G.,& Mead, N.R., (2008). Software Security Engineering: A Guide for Project Managers. Upper Saddle River, NJ: Addison Wesley Professional.

[2] B. Hirsch and J. W. P. Ng, "Education beyond the cloud: Anytime-anywhere learning in a smart campus environment," 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, 2011, pp. 718-723.

[3] CAK. (2008). Kenya Internet Market Study Report. Retrieved from www.ca.go.ke on December 16th 2015.

[4] Dearbhla M. (2010). Kenya Poised for Huge Growth in Mobile Services, Pyramid Research Projects. Retrieved December 18th, 2015. http://www.pyramidresearch.com/downloads.htm?id=18&sc=PR031609_CIRK

[5] Davcev, D., & Kitanov, S. (2012). Mobile Cloud Computing Environment as a Support for Mobile Learning. In Cloud Computing 2012, 3rd International Conference on Cloud Computing, GRIDs, and Virtualization, 99-105.

[6] Dinh, H. T., Lee, C., Niyato, D. and Wang, P. (2013), A survey of mobile cloud computing: architecture, applications, and approaches. Wirel. Commun. Mob. Comput., 13: 1587–1611. doi:10.1002/wcm.1203.

[7] ENISA. (2010). Smartphone: Information security risks, opportunities and recommendations for users Smartphone. Eurostats. Retrieved September 19th, 2015 from http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_ statistics_on_the_use_by_enterprises.

[8] Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2012). How to design and evaluate research in education (8th ed.). New York: Mc Graw HIll.

[9] Gartner. (2012, October). Mobile Cloud Computing Retrieved from http://www.gartner.com/newsroom/id/2213115 on October 13th, 2015.

[10] Gu Q., Guirguis M. (2014) Secure Mobile Cloud Computing and Security Issues. In: Han K., Choi BY., Song S. (eds) High Performance Cloud Auditing and Applications. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-3296-8_3.

[11] Information Systems, Audit and Control Association inc (ISACA). (2010). ISACA. International Data Cooperation: 2010 Consumerization of IT study: Closing the consumerization gap. International Data Cooperation Retrieved from www.isaca.org on December 28th 2015, from www.isaca.org.

[12] ISACA. (2011). IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. Information Systems, Audit and Control Association inc (ISACA).

[13] Jeon W., Kim J., Lee Y., Won D. (2011) A Practical Analysis of Smartphone Security. In: Smith M.J., Salvendy G. (eds) Human Interface and the Management of Information. Interacting with Information. Human Interface 2011. Lecture Notes in Computer Science, vol 6771. Springer, Berlin, Heidelberg.

[14] Kawaljeet, K., & Gurjit, S. B. (2015). Major security issues and challenges in mobile cloud computing: A review. International Journal for Multi Disciplinary Engineering and Business Management.

[15] Khan, A. N., M, L., Mat, K., Samee, U., & Sajjad, A. (2012). Towards secure mobile cloud computing: A survey. Future Generation Computer Systems.

[16] Khan, S., Hasan, M. and Clement, C. (2012). Barriers to the introduction of ICT into education in developing countries: The example of Bangladesh. International Journal of Instruction, Vol. 5(2), pp. 61-80. Retrieved on November 15, 2015 on http://www.e-iji.net/dosyalar/iji_2012_2_4.pdf.
[17] Morgan,S.(2010), Mobile web statistics, www.morganstanley.com. Retrieved from http://mashable.com/2010/04/13/mobile-web-stats/ on September 28th, 2015.
[18] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck and C. Wolf, "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," 2011 IEEE Symposium on Security and Privacy, Berkeley, CA, 2011, pp. 96-111.
[19] doi: 10.1109/SP.2011.29
[20] Narcisi, G.(2012). HIPAA-compliant data center: secure with business associate agreement. Retrieved from Techtarget: http://searchtelecom.techtarget.com/news/2240165182/HIPAA-compliant-data-center-Secure-with-Business-Associate-Agreement on May 11th, 2015.
[21] NESC. (2007). Kenya Vision 2030: A globally competitive and prosperous Kenya. National Economic and Social Council of Kenya.
[22] Olayinka, O., Hani, P., & Silas, V. (2015). A New Secure Mobile Cloud Architecture. IJCSI International Journal of Computer Science Issues, 12(2).
[23] Palmer, R., & Dodson, L. (2011). Distance learning in the cloud: Using 3G enabled mobile computing to support rural medical education. Journal of the Research Center for Educational Technology, 7(1), 106-116.
[24] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, Ivona Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 2009, 25(6), 599-616, https://doi.org/10.1016/j.future.2008.12.001.
[25] Rao, N. M., Sasidhar, C., & Kumar, V. S. (2010). Cloud computing through mobilelearning. Computing, 1(6).
[26] Rittinghouse, J. W., & Ransome, J. F. (2009). Cloud security challenges. Cloud Computing: Implementation, Management, and Security, 158-161.
[27] Rugg, G., & Petre, M. (2007). A gentle guide to research methods. Poland: OZ Graf.S.A
[28] SANS (2010). Information Security Resources. Retrieved 2015, from SANS Information Security Resources: http://www.sans.org/information_security.php.
[29] Satyanarayanan, Mahadev (2010) Mobile Computing: The next decade proceedings of the 1st ACM Workshop on Mobile Cloud Computing, Social Networks and Beyond, San Francisco, California, http://doi.acm.org/10.1145/1810931.1810936, ACM, New York, NY, USA
[30] Sekaran, U, & Bougie, R. (2010). Research methods for business: A skill building approach 1 (5) West Sussex, UK: John Wiley & Sons Ltd.
[31] Sultan, N, (2010) Cloud computing for education: A new dawn? International Journal of Information Management, 30(2), 109-116, https://doi.org/10.1016/j.ijinfomgt.2009.09.004.
[32] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34(1), 2011, Pages 1-11, https://doi.org/10.1016/j.jnca.2010.07.006.
[33] Sophos. (2010). Security Threat Report. Retrieved 2015, from http://www.sophos.com: http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf.
[34] Woodill, G. (2010). The mobile learning edge: Tools and technologies for developing your teams. McGraw-Hill.
[35] Yamane, Taro. (1967). Statistics: An Introductory Analysis, 2nd Ed., New York: Harper and Row.