UWS UNIVERSITY OF THE WEST of SCOTLAND

School of Computing, Engineering & Physical Sciences

Computing and Information Systems Journal

Vol 22, No 1, 2018

Edited by Abel Usoro

www.uws.ac.uk

Computing and Information Systems is published normally three times per year, in February, May, and October, by the University of the West of Scotland.

From the next issue the editorial address is Dr Abel Usoro, School of Computing, University of Paisley PA1 2BE; tel (+44) 141 848 3959; fax (+44) 141 848 3542, e-mail: cis@uws.ac.uk or abel.usoro@uws.ac.uk.

Editorial Policy

Computing and Information Systems offers an opportunity for the development of novel approaches, and the reinterpretation and further development of traditional methodologies taking into account the rate of change in computing technology, and its usage and impact in organisations.

Computing and Information Systems welcomes articles and short communications in a range of disciplines:

- Organisational Information Systems
- Computational Intelligence
- E-Business
- Knowledge and Information Management
- Interactive and Strategic Systems
- Engineering
- E-Learning
- Cloud Computing
- Computing Science

The website for Computing and Information Systems is http://cis.uws.ac.uk

UWS UNIVERSITY OF THE WEST of SCOTLAND

Printed by Printing Services, University of the West of Scotland

The Threat of Split-Personality Android Malware on Developing Economy

Oluwakemi Christiana Abikoye
Department of Computer Science,
University of Ilorin,
Ilorin, Nigeria
kemi_adeoye@yahoo.com

Gyunka Benjamin Aruwa
Department of Computer Science,
University of Ilorin,
Ilorin, Nigeria
gyunkson@gmail.com

ABSTRACT

Purpose: Android Smartphones and Tablets are massively proliferating into every sector of national economies. The developed economies are well advanced in making preparations against any eventualities and security challenges that might arise with the adoption of these technologies. Developing economies on the other hand are not well ready to face the different devastating challenges. This work seeks to critically evaluate the security threats associated with Android malware, especially the awareness rate of Android users to the existence of Android malware and the associated cyber threats on growing economies.

Design/Methodology/Approach: A survey was adopted and secondary literatures were critically analyzed to fulfill the objectives of the research.

Findings: The findings revealed very low rate of Android malware and cyber threats awareness amongst users in developing economies.

Practical Implications: With the evasive and sophisticated nature of malware, such as the Split-personality malwares, low or zero awareness rates of malware threats and the acceptable cybersecurity behaviours and practices can have a huge negative impact on the growth of any economy**.**

Originality: The results and findings in this study were primarily derived and analyzed by the Authors. It is a unique study in the field of Android malware research.

Keywords: *Android; Split-Personality Malware; Cyber Security; Smartphones; analysis systems; economy*

Paper Type: *Research Paper*

1 Introduction

Cyber security awareness and the consciousness of mobile malware threats have received little or no major attention in many economies, especially the developing ones. The very high and uncontrollable influx of technological devices, especially the Android Smartphones, into both the developed and the developing economics has been greatly alarming (Feng et al., 2014). The economies of Nations in the twenty-first century massively depend on the different technological platforms as a major pivot on which their growths and advancements are anchored. Different marketing activities, commerce, banking, and vital information storage are now almost completely being carried out via the different technological devices. Although developed economies rapidly embrace new technologies and introduce them into the operations of their markets, they also thrive in making policies and codes of practice for the safe use of these technologies. This they do by sponsoring researches and devising different methodologies to stand ready to overcome any challenges that might come up as the result of the deployment of these technological devices. On the contrary, Developing Economies are usually very quick at adopting and deploying new technologies but they acutely lack the appropriate preparations to manage and withstand challenges that arises with the use of the technologies (Malwarebytes Labs, 2017).

Most users of these devices are unaware that, holding a Smartphone which has full internet access activated, creates a complete open access to the whole world or the whole world having a complete and open access to the device (Kende, 2014). Malicious applications provide

an easy and vulnerable access that enables a remote control of these devices from anywhere in the world. Internet access in developing economies has not been very sustainable at some locations (Kende, 2014); this can be considered as an advantage when it comes to cyber attacks, but with the rapid introduction and adoption of open internet access comes greater vulnerabilities to be exploited by cyber attackers. The diffusion of Android devices into the different sectors of developing economies is at an exponential rate and this has made them become prime targets for cyber attackers (Snell, 2016). The implementation of e-Banking, e-Commerce and lots more of classified and sensitive activities has exposed most economies to cyber attacks. This can be more catastrophic for developing economies who are unprepared to prevent and manage such attacks (Ian, 2017).

Majority of the attacks launched against the Android platform are malware based (Snell, 2016; Raveendranath et al., 2014). Malware is a term used to describe a malicious application or software. Android malware was first introduced in the year 2010 and since then there has been a record of over 300 Android malware families in circulation (Sophos, 2014). Some dangerous Android malware includes Ginmaster (Sophos, 2014), Stagefright (collections of bugs or code errors) released in 2015 (Snell, 2016)and Judy Malware (Team, 2017). The field of Android malware has seen plenty of security researches which have been conducted for the reasons of seeking counter measures against the activities of these malwares (Arp et al., 2014; Arzt et al., 2014; Lindorfer et al., 2014; Narayanan et al., 2016; Raveendranath et al., 2014; Spreitzenbarth et al., 2013). Although most of these researches have yielded profound results in coming out with reactive detection measures, yet Android malware are increasingly growing in sophistications and innovative techniques to remain undetected.

A particular family of Android malware, known as the Split-Personality malware, has recently become a contending issue of great concern to the Android security research community. This family of malware have a dual behavioural capacity; they can appear to be benign during installations or analysis processes and then become malicious once installed and executed on a real physical device. This work will critically look at Android malware and the rate at which Android users are aware of the existence of malware and the threats they pose to the growths of developing economies.

2 The Making of Android Malware

Developing Android malware is not an abstract concept; malware appear mostly in guise as legitimate applications. This means that malicious developers embed malicious codes or payloads and compile them into applications that are usually of high interest to a particular target group of users. The altered applications could fall in the group of banking apps, e-commerce apps, entertainment apps (games, audio, video, photos, etc.), location apps and lots more. Sometimes, the malware authors only extract a legitimate application, employ the method of reverse engineering to alter either the application's code, permissions or some API calls in order to inject their desired intents. In order to understand the formation of an Android malware, it is imperative to know what a typical Android apk file looks like and the different components of interest targeted by malware authors. Reverse engineering is a cardinal method in the process of decompiling and recompiling an Android .apk file.

a. The Android Application Package (APK)

Android applications are also called apk files; this is due to the reason that these applications are created and compiled into Android Package (APK) with a .apk extention format (Rovelli & Engineering, 2014; Zhauniarovich, 2014). These files are similar to .zip files in Windows and Linux.

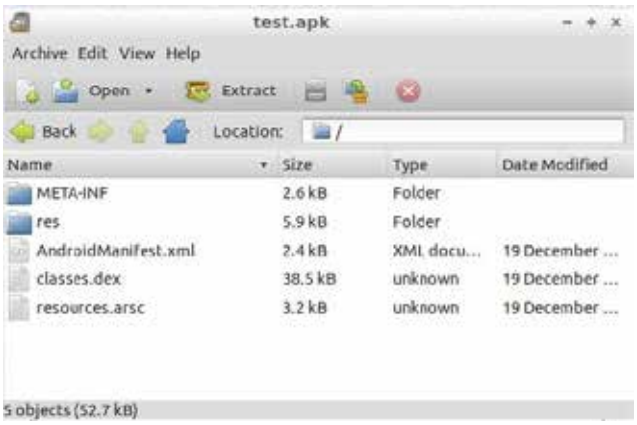


Figure 1: An APK unzipped file displaying its contents (Fora, 2014)

The .apk can be changed to .zip and can be opened in Windows or Linux (Fora, 2014). Figure 1 gives a clear picture of what a typical Android apk file looks like and the basic contents. APK files are shipped containing

metadata, GUI layout definitions, Dalvik and native code and other resources the app will need (Hahn, Protsenko, & Müller, 2016).
The content of an APK consists of Dalvik executables, resources, native libraries and a manifest file; and is usually signed by the developer of the application using self-signed certificate (Rovelli & Engineering, 2014; Zhauniarovich, 2014). The contents are as explained below:

i. META-INF: This a directory which contains MANIFEST.MF (i.e., the Manifest file); CERT.RSA (i.e., the certification of the application); CERT.SF (this is the list of resources and SHA-1 of the corresponding lines in the MANIFEST.MF file)
ii. res: this is a directory that contains the resources that are not compiled into resources.arsc. This includes icons, images, music etc.
iii. AndroidManifest.xml: this file describes the name, version, access rights (permissions), and reference library files for the application. It also contains four basic components which are Activities, Services, Broadcast Receivers and Content Providers (Yerima et al., 2016). Without this file and its contents, an application cannot be installed or be executed (Shah & Researcher, 2011; Zhauniarovich, 2014).
iv. classes.dex: this file is compiled in the dex format so as to enable its execution in the Dalvik Virtual Machine (Dalvik VM). The file contains the main working code of the application. That is, the payloads of an application is created and defined in classes.dex file.
v. resources.arsc: this file contains pre-compiled resources such as XML.

Other components that may be found in an apk file include *lib* and *akssets*. *lib* is a directory that contains compiled code which are specific to a software layer of a processor. Some sub-folders contained in the *lib* folder include *armeabi*, *armeabi-v7a*, *x86*, and *mips*. The *classes.dex* and *AndroidManifest.xml* are the most delicate and important components of the APK file which are usually the high targets of malware creators (Shah & Researcher, 2011; Tchakounté & Dayang, 2013).

b. Reverse Engineering

Reverse engineering in computing is a procedure which enables the analyzing and understanding of how a system works and the interrelationships between its components and then reusing the gained information to develop representations of the system in a different form or a higher level of abstraction (Aguilera, 2013). In Android, reverse engineering can be used to read an app's code, find vulnerabilities in the code, search for sensitive data hardcoded in the code, and in the analysis of malware or in modifying the functionality of an existing application. It is a static method of analyzing an apk file as can be seen in Figure 2.

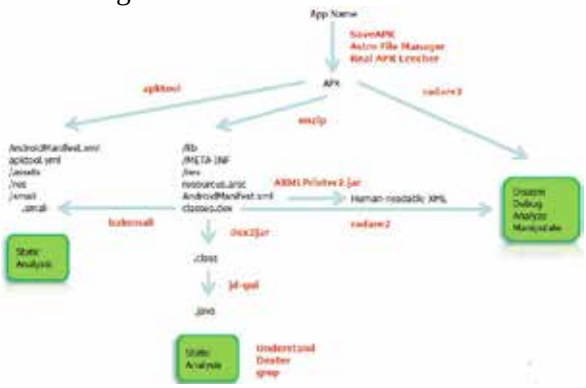


Figure 2: Android APK Reverse Engineering Steps (Aguilera, 2013)

This implies that it is a process in which the apk file is decompiled or disassembled and the different components are extracted and converted into human readable formats for the purpose of research and investigations. This same procedure is also being utilized by malware authors to compromise legitimate applications by injecting malicious codes into them. Some very commonly used tools for reverse engineering include:

i. *AXML2jar*: helps in converting the manifest file into readable format
ii. *ApkTool:* helps in decoding resources to original form and can be used to rebuild it back after modification. It is also useful for transforming binary Dalvik bytecode (classes.dex) into Smali source

iii. *Dex2Jar:* enables the conversion of Dalvik bytecode (DEX) to java bytecode (JAR)
iv. *Androguard:* used for disassembling and decompiling Android APK files
v. *Android SDK:* A development kit made for developers to create applications for the Android platform
vi. *Smali/Baksmali:* it is disassembled for the dex format used by Dalvik so it will be used to disassemble the .dex file Android SDK,
vii. APK Inspectors
viii. *Jd*-gui: helps in converting a .jar file to .java
ix. AXMLPrinter2: converts Android binary XML to human-readable XML

3 Split-Personality Android Malware

This family of malware are very crafty and cunning in nature and they are characterized by a dual personality (Aquilina, 2015; Richter, 2015). They are highly sophisticated in their concealment techniques which make them escape most dynamic analysis frameworks. They are also known as VM-aware malware (Kirat et al., 2011). These categories of malwares possess a strong fingerprinting characteristic which enables them to detect any analysis environment upon which they are executed, and then hide their true nature, pretending to be benign applications. This same fingerprinting characteristic also enables them to know when they are running on a real physical device, which makes them take up a malicious form, revealing their true nature. Fingerprinting techniques involve checking for specific artifacts, such as some specific registry keys, background processes, function hooks, or IP addresses that are specific to a known analysis tool (Maier et al., 2014). The malware authors would usually have a pre-knowledge of these artifacts before they are able to develop malwares that can withstand them through fingerprinting techniques. The attacks lunched by Split-personality malware usually begin by first putting on a dual behaviour, benign and malicious, which are totally distinct and independent from each other. Whenever they sense the presence of a security scanner, they trick it by showing up a benign behaviour, but the reverse is the case when they sense the presence of a true physical device (Maier et al., 2014).

The activities of the Split-personality malware are interwoven between loading malicious code and loading malicious script when run on a physical device. These category of malwares sometimes use drive-by-downloads in the form of plug-ins, extensions, or updates to trick the user into downloading the intended malicious payloads (Raveendranath et al., 2014). AnserverBot, an Android malware, exhibits these characteristics by fetching and executing malicious payload at run time on physical devices (Yerima et al., 2013). Malware sophistications is developed through polymorphism, increased code obfuscation, malicious payloads encryption, as well as through stealthy command and control communications with remote servers (Narayanan et al., 2016). This makes these class of malware extremely difficult to be detected by traditional detection systems (Raveendranath et al., 2014; Zhauniarovich, 2014). The goal of the concealment strategies is to enable the malware survive longer without detection in order to have ample available time to replicate and infect more devices (Aquilina, 2015).

4 Android Malware Detection Techniques

Contending Android malware employs two major methodologies and these are static and dynamic analysis techniques. Lots of other advanced methodologies, such as the hybrid and machine learning approaches, span from these two main methods. The robustness or effectiveness of a method lies mainly in the ways or the environments on which either or both of the two main methods are applied.

a. Static Analysis

The method of static malware analysis is also known as code analysis. It is a procedure of studying the underlying code or components of an application without necessarily executing the application (Richter, 2015). In Android, the process is used to study the components of the AndroidManifest.xml file and the byte code of the classes.dex file (Dunham et al., 2014). Static analysis can easily be tricked and bypassed by simple obfuscation techniques and can thus not protect against various polymorphic and

metamorphic malwares. However, static analysis technique does not provide an enabling environment for malware to fingerprint the analysis platform or modify its behaviour in order to avoid detection (Apvrille & Strazzere, 2012). For this reason, machine learning technique uses static features for malware analysis. Static code analyzers are also deployed in malware analysis frameworks like Tracedroid, Andrubis, Sanddroid, Drebin (Arp et al., 2014), and Marvin (Lindorfer et al., 2015).

b. Dynamic Analysis

Dynamic analysis approach involves practical execution of an application in a controlled environment for the purpose of studying the behaviour of such an applications (van der Veen et al., 2013). Dynamic analysis method can also be referred to a sandboxing system. Sandboxing is a process of virtualization that tries to simulate a real physical device with little or no traces of virtualization (Bläsing et al., 2010; Neuner et al., 2014). Under this method, the analysis environment is expected to be indistinguishable from the real physical device so as to be able to trick a malware sample into believing that it is being executed on a real physical device. This will make the malware reveal its real identity or characteristics which will make its detection lots easier. However, sandboxing system has failed to completely mimic a real physical device, hence the continuous challenge of their inability to curb these sophisticated class of malware (Richter, 2015).

Sandboxing analysis solutions are mostly automated and they have different modes of operations distinct from one another, each having its analysis capacity and the unique features it is built to look for as red flags during analysis, but there are malware that still cannot be detected by these known solutions (Maier et al., 2015; Neuner et al., 2014; Richter, 2015). Dynamic analysis method is largely known to be highly resource intensive and can be affected by methods of runtime detection (Dunham et al., 2014; Raveendranath et al., 2014). Some dynamic malware analysis systems available include Andlantis (Bierma et al., 2014), XManDroid (Bugiel et al., 2011), TaintDroid (Enck et al., 2014; Richter, 2015), and FlowDroid (Arzt et al., 2014).

5 Machine Learning Approach

Machine Learning is a system or technique in which computers are made to learn from past experiences (existing data sets) in order to be able to make a generalized prediction or decision on new data sets that maybe introduced in the future. It is a procedure in which algorithms are developed and trained to make prediction from data. Three main types of Machine Learning exist and they are the supervised learning, the unsupervised learning, and the reinforcement learning. Supervised learning deploys classification and regression algorithm methods; unsupervised learning adopts the methods of clustering algorithms, while reinforcement learning operates by a principle of reward. For malware analysis, the classification methods of supervised learning are mostly suitable and widely deployed because the learning classifiers have notably become a leading method for the analysis of Smartphones malware (Amos, Turner, & White, 2013).

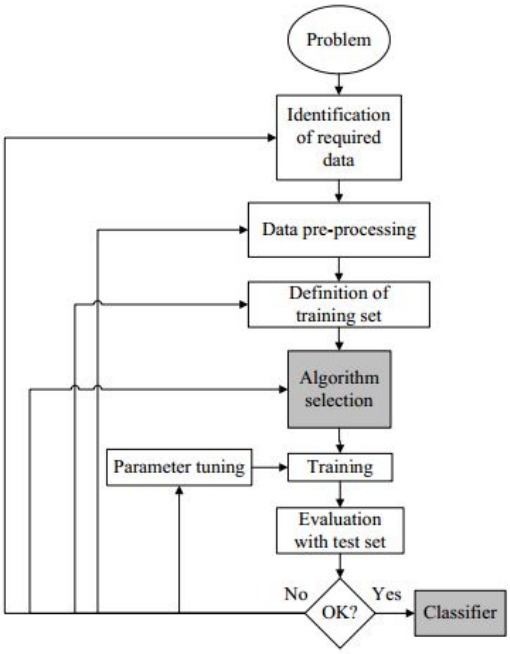


Figure 3: Supervised Machine Learning Process (Kotsiantis, 2007)

For defeating Android split-personality malware and any other evasive malware, the Bare-metal analysis method (Kirat et al., 2011; Kirat et al., 2014) and the Machine Learning method (Arp et al., 2014) are the two leading approaches proposed. However, the bare-metal approach for Android split-personality malware analysis has not yet received any major attention due to lots

of technical complexities (Maier et al., 2014), except for the only attempt by Mutti et al., (2015) which produced BareDroid as a bare-metal malware analysis approach for the Android platform. Machine Learning, on the other hand, is highly scalable and adaptable for deployment on any platform, either mobile or desktops. The deployment of Machine Learning in the detection and analysis of Android malware largely depends on the static features of an application, either benign or malicious (Hahn et al., 2016). Figure 3 shows a flowchart which demonstrates the different stages taken for malware analysis using supervised machine learning method.

6 Methodology

In order to ascertain the level of Android malware awareness in a developing economy, a survey was conducted in Kano State, one of the major Commercial Cities, asides Lagos and Port Harcourt, of Nigeria. The slogan for Kano State is 'Centre of Commerce' and it is located in the Northern region of the Country. The period of the survey was between July and August 2017.

6.1 Data Collection

The survey responses were collected from a random sampled population of 200 people, across gender, of different ages - the young (ages 15 - 40), the mid-aged (ages 41 - 60), and the elderly (ages 61 - 80) both on the street and in public offices. The data was collected from the different categories and was analyzed using Microsoft Excel. Some of the major factors or indices considered in the survey are as follows:

i. Do you know there is anything called malware or malicious applications for Android?
ii. Do you know what a third party application is?
iii. How often do you install applications from a third party site (i.e., applications not gotten from Google Play Store)?
iv. Do you know the risk of third party sites?
v. How often do you install application from Google Play Store?
vi. Do you have an Anti-virus installed in your Smartphone and do you know what function it performs?
vii. Do you usually take the time to check carefully all the requested permissions during application installations?
viii. Do you know what cyber attack is all about?
ix. Do you use your Smartphone for online Banking and e-commerce?
x. Do you know the kind of sensitive information that can be stolen from your Smartphone?

7 Summary and Analysis of the Results

Table 1: Do you know there is anything called Android Malware?

ANSWER CHOICES	RESPONSES	
Yes	70	35%
No	130	65%
TOTAL	200	100%

Table 2: Do you know what a third party application is?

ANSWER CHOICES	RESPONSES	
Yes	40	20%
No	100	50%
Don't Care	60	30%
TOTAL	200	100%

Table 3: How often do you install applications from a third party site (i.e., applications not gotten from Google Play Store)?

ANSWER CHOICES	RESPONSES	
Sometimes	40	20%
Never	35	17.5%
Anywhere free apps available	125	62.5%
TOTAL	200	100%

Table 4: Do you know the risk of third party sites?

ANSWER CHOICES	RESPONSES	
Yes	36	18%
No	164	82%
TOTAL	200	100%

Table 5: How often do you install application from Google Play Store?

ANSWER CHOICES	RESPONSES	
Always	112	56%
Some times	39	19.5%
When necessary	49	24.5%
TOTAL	200	100%

Table 6: Do you have an Anti-virus installed in your Smartphone and do you know what function it performs?

ANSWER CHOICES	RESPONSES	
Yes	68	34%
No	33	16.5%
I don't know	99	49.5%
TOTAL	200	100%

Table 7: Do you usually take the time to check carefully all the requested permissions during application installations?

ANSWER CHOICES	RESPONSES	
Yes	36	18%
No/I don't care	164	82%
TOTAL	200	100%

Table 8: Do you know what cyber attack is all about?

ANSWER CHOICES	RESPONSES	
Yes	23	11.5%
No	177	88.5%
TOTAL	200	100%

Table 9: Do you use your Smartphone for online Banking and e-commerce?

ANSWER CHOICES	RESPONSES	
Yes	128	64%
No	33	16.5%
Some Times	39	19.5%
TOTAL	200	100%

Table 10: Do you know the kind of sensitive information that can be stolen from your Smartphone?

ANSWER CHOICES	RESPONSES	
Yes	31	15.5%
No	113	56.5%
Nothing in my Phone that can be Stolen	56	28%
TOTAL	200	100%

8 Discussion

From all the responses received for each question, the 'yes' or 'positive' responses shows the total awareness rate of the populace to the existence of Android malware and cyber threats.

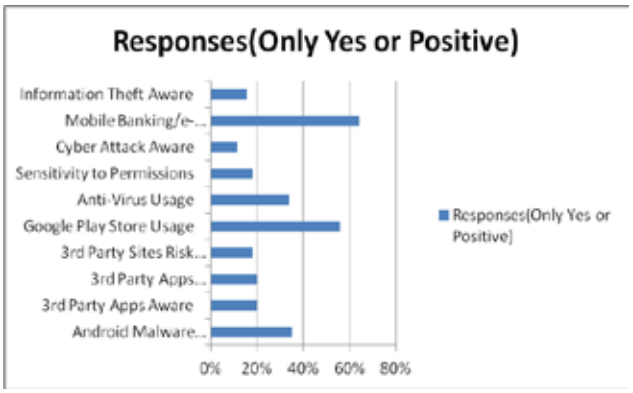


Figure 4: Cumulative Android malware and Cyber Threats awareness rate

The awareness rate is very low as regards to malware existence and the risks of visiting a third party site even though Smartphones are highly used for online transactions such as mobile banking and e-commerce. These activities massively expose the different users to cyber threat without the appropriate security measures for resource protection. Massive malware attacks can exploit the unawareness of Android users to basic security policies. Figure 4 shows the very low awareness rate to Android malware and vulnerabilities that can be exploited on the Android device.

9 Implication on Developing Economy

Developing economies are always thriving to attain a robust and a sustainable position with a competitive speed. This increases their readiness to quickly embrace any system or technology that seems viable in enhancing the achievement

of their goal even though they do not give much thought on the resultant negative implications. Android devices have penetrated widely into developing economies and their spread has massively boosted the penetration of open internet access even into deep rural areas. As a result, lots of activities have been taken over by the internet. Shops are moving online, there is now online banking, electronic mails, online payments, and lots of other human private and public activities have found an easy platform on the internet. People can now buy and sale things online, transfer cash electronically, pay bills, book airlines, and store vital and sensitive information online.

Although all these advancements are highly welcoming, especially in the way they are boosting the economy and commerce, they also have created openings through which the economy can be sabotaged by competitors, cyber thieves etc. Not many users of the Android device are aware of the different activities and classes of malware in existent, especially in the Developing Economy. Some are content with having antivirus software run on their devices while majority others do not really care or do not see the need.

The practice of cyber security awareness is not given any encouraging attention amongst the workforce, the business class, and the common users of Smart devices in Developing Economies. So, the largest proportion of the Developing Economy population is ignorant of basic cyber security behaviours, thus creating a huge cyber vulnerability (Mittu & Lawless, 2015). For the few that understand the importance of protecting against Android malware using the different detection mechanisms available such as the anti-virus, research has also shown that such detection systems do not provide real time detection and so it leaves most of these users vulnerable to malware attacks of every kinds (Fedler, Schütte, & Kulicke, 2013; Maier et al, 2014). Split-personality Android malware are a growing concern, especially for developing Economies, due to their subtle nature of escaping most of the available detection systems (Enck et al, 2011). For the developing Economies to grow and be placed in the same position with advanced Economies, serious attention will have to be given to research into ways of having safe e-commerce and e-banking systems that are free from malware and cyber attacks of any kinds. Android malware research will have to be encouraged at different levels of learning.

10 Conclusion

In this article, it has been discussed that cyber attacks succeed easily mostly because of the porous ways the highly proliferated Android devices are being utilized which makes them vulnerable to malware activities. It has also been noted that majority of the malware detection systems available do not provide absolute protection as they cannot protect on real time. These limitations in the detection systems allow lots of malware to be undetected, especially the split-personality malware.

It has thus become very necessary that if developing economies must thrive to a state of robustness, they must make sufficient provision for continuous counter malware researches, spend time and resources in taking proactive measures to sensitize and make aware the entire population regarding acceptable cyber security behaviour and practices and the dangers of malware attacks. The consequences of split-personality malware can be drastic on the economy if such appropriate steps are not taken to contend them.

References

Aguilera, V. (2013). Android reverse engineering: understanding third-party applications. In OWASP EU Tour. Bucharest: The OWASP Foundation. Retrieved on 19th July 2017 from https://www.slideshare.net/ISecAuditors/android-reverse-engineering?from_action=save

Amos, B., Turner, H., & White, J. (2013). Applying machine learning classifiers to dynamic android malware detection at scale. *2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013*, pp. 1666–1671.

Apvrille, A., & Strazzere, T. (2012). Reducing the window of opportunity for Android malware Gotta catch ’em all. *Journal in Computer Virology*, Vol. 8, No. 1–2, pp. 61–71.

Aquilina, N. (2015). Cross-Platform Malware Contamination Cross. Tech. rep. (Vol. 11). London: RHUL. Retrieved on 10th April 2016 from https://www.royalholloway.ac.uk/isg/docu

ments/pdf/technicalreports/2015/rhul-isg-2015-11.pdf.

Arp, D., Spreitzenbarth, M., Malte, H., Gascon, H., & Rieck, K. (2014). Drebin: Effective and Explainable Detection of Android Malware in Your Pocket. *Symposium on Network and Distributed System Security (NDSS)*, (February), pp. 23–26.

Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., Traon, Yves Le, Octeau, D., Mcdaniel, P. (2014). FlowDroid : Precise Context , Flow , Field , Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps. *PLDI '14 Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation*, pp. 259–269.

Bierma, M., Gustafson, E., Erickson, J., Fritz, D., & Choe, Y. R. (2014). Andlantis : Large-scale Android Dynamic Analysis. *Proceedings of the 3rd IEEE Mobile Security Technologies Conference (MoST)*.

Bläsing, T., Batyuk, L., Schmidt, A. D., Camtepe, S. A., & Albayrak, S. (2010). An android application sandbox system for suspicious software detection. *Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software, Malware 2010*, pp. 55–62.

Bugiel, S., Davi, L., Dmitrienko, A., Fischer, T., & Sadeghi, A. (2011). XManDroid: A New Android Evolution to Mitigate Privilege Escalation Attacks. *Technische Universität Darmstadt, Technical Report*, pp. 1–18.

Check Point Mobile Research Team (2017). The Judy Malware: Possibly the largest malware campaign found on Google Play. Retrieved on 8th July 2017 from blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

Dunham, K., Hartman, S., Morales, J. A., Quintans, M., & Strazzere, T. (2014). *Android malware and analysis*. New York: CRC Press.

Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2014). TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. *Communications of the ACM*, Vol. 57, No. 3), pp. 99–106.

Fedler, R., Schütte, J., & Kulicke, M. (2013). On the Effectiveness of Malware Protection on Android. Tech. rep. Berlin: Fraunhofer AISEC.

Feng, Y., Anand, S., Dillig, I., & Aiken, A. (2014). Apposcopy : Semantics-Based Detection of Android Malware Through Static Analysis. In *Proceedings of the ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE'14)*, pp. 16–22.

Fora, P. O. (2014). Beginners Guide to Reverse Engineering Android Apps. *RSA Conference*, pp. 21–22.

Hahn, S., Protsenko, M., & Müller, T. (2016). Comparative evaluation of machine learning-based malware detection on Android. *Sicherheit 2016: Sicherheit, Schutz Und Zuverl{ä}ssigkeit, Beitr{ä}ge Der 8. Jahrestagung Des Fachbereichs Sicherheit Der Gesellschaft F{ü}r Informatik e.V. (GI), 5-7 April 2016, Bonn*, pp. 79–88.

Ian, B. (2017). 2016's top malware threats show a shift in attack patterns. Retrieved on 4th April 2017 from https://betanews.com/2017/01/31/malware-threat-pattern-shift/

Kende, M. (2014). Internet Society Global Internet Report 2014. *Internet Society*, 146. Retrieved on 7th May 2015 from http://www.internetsociety.org/doc/global-internet-report%5Cnhttps://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014.pdf

Kirat, D., Vigna, G., & Kruegel, C. (2011). BareBox: efficient malware analysis on bare-metal. *Proceedings of the 27th Annual Computer Security Applications Conference*, pp. 403–412.

Kirat, D., Vigna, G., & Kruegel, C. (2014). BareCloud: Bare-metal Analysis-based Evasive Malware Detection. *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 287–301.

Kotsiantis, S. B. (2007). Supervised machine learning: A review of classification techniques. *Informatica*, Vol. 31, pp. 249–268.

Lindorfer, M., Neugschwandtner, M., & Platzer, C. (2015). MARVIN: Efficient and Comprehensive Mobile App Classification through Static and Dynamic Analysis. *In 2015 IEEE 39th Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2, pp 422–433. *IEEE.*

Lindorfer, M., Volanis, S., Sisto, A., Neugschwandtner, M., Athanasopoulos, E., Maggi, F., Platzer, C., Zanero, S., Ioannidis, S. (2014). AndRadar: Fast discovery of Android applications in alternative markets. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (Vol. 8550 LNCS, pp. 51–71). Cham: Springer.

Maier, Dominik; Müller, Tilo; Protsenko, M. (2014). Divide-and-conquer: Why android malware cannot be stopped. *In 9th IEEE International Conference on Availability, Reliability and Security (ARES), 2014*, pp. 1–10.

Malwarebyte Labs. (2017). 2017 *State of Malware Report.* Retreived on 2nd August 2017 from https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf

Maier, D., Protsenko, M., & Müller, T. (2015). A game of Droid and Mouse: The threat of split-personality malware on Android. *Computers & Security*, pp. 2–15.

Maier, Dominik; Müller, Tilo; Protsenko, M. (2014). Divide-and-conquer: Why android malware cannot be stopped. 9th IEEE International Conference on Availability, Reliability and Security (ARES), 2014, pp. 1–10.

Malwarebytes Labs. (2017). 2017 State of Malware Report.

Mittu, R., & Lawless, W. F. (2015). Human Factors in Cybersecurity and the Role for AI. In *Foundations of Autonomy and Its (Cyber) Threats: From Individual to Interdependence, AAAI Spring Symposium Series*, pp. 39–43.

Mutti, S., Fratantonio, Y., Bianchi, A., Invernizzi, L., Corbetta, J., Kirat, D., Kruegel, C., Vigna, G. (2015). BareDroid. *Proceedings of the 31st Annual Computer Security Applications Conference on - ACSAC 2015*, pp. 71–80.

Narayanan, A., Yang, L., Chen, L., & Jinliang, L. (2016). Adaptive and scalable android malware detection through online learning. *Ijcnn 2016*, pp. 2484–2491.

Neuner, S., Veen, V. Van Der, & Lindorfer, M. (2014). Enter Sandbox: Android Sandbox Comparison. *3rd IEEE Mobile Security Technologies Workshop*, (October).

Raveendranath, R., Rajamani, V., Babu, A. J., & Datta, S. K. (2014). Android malware attacks and countermeasures: Current and future directions. *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies, ICCICCT 2014*, pp. 137–143.

Richter, L. (2015). Common Weaknesses of Android Malware Analysis Frameworks. *Ayeks.de*, pp. 1–10.

Rovelli, P. (2014). Developing a Next-Generation Mobile Security Solution for Android. MSc Thesis, Reykjavík University. Retrieved on 3rd June 2016 from https://skemman.is/bitstream/1946/19500/1/Developing%20a%20next-generation%20Mobile%20Security%20solution%20for%20Android%20-%20Paolo%20Rovelli.pdf

Shah, R. (2011). Analyzing and Dissecting Android Applications for Security defects and Vulnerabilities. Retrieved on 10th March 2017 from https://www.helpnetsecurity.com/dl/articles/Blueinfy_Rushil_ScanDroid_Paper.pdf

Snell, B. (2016). Mobile Threat Report: What's on the Horizon for 2016. In *Intel Security and McAfee*. Retrieved on 18th February 2017 from http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

Sophos. (2014). Security Threat Report 2014. *Security*, pp. 1–34. Retrieved on 22nd July 2017 from https://www.sophos.com/en-us/medialibrary/pdfs/other/sophos-security-threat-report-2014.pdf

Spreitzenbarth, M., Freiling, F. C., Echtler, F., Schreck, T., & Hoffmann, J. (2013). Mobile-sandbox: Having a Deeper Look into Android Applications. *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, pp. 1808–1815.

Tchakounté, F., & Dayang, P. (2013). System Calls Analysis of Malwares on Android. *International Journal of Science and Technology*, *2*(9), pp. 669–674.

van der Veen, V., Bos, H., & Rossow, C. (2013). Dynamic Analysis of Android Malware. Retrieved on 12th February 2017 from https://www.vvdveen.com/publications/MSc.pdf

W.Enck, Octeau, D., McDaniel, P., & Chauhuri, S. (2011). A Study of Android Application Security. *Proc. ACM USENIX*, (August).

Yerima, S. Y., Sezer, S., & Muttik, I. (2013). A

New Android Malware Detection Approach Using Bayesian Classification. In *In Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on* (pp. 121–128).

Yerima, S. Y., Sezer, S., & Muttik, I. (2016). Android Malware Detection Using Parallel Machine Learning Classifiers. *2014 Eighth International Conference on Next Generation Mobile Apps, Services and Technologies*, (Ngmast), pp. 37–42.

Zhauniarovich, Y. (2014). *Android TM Security (and Not) Internals (ASANI Book)*.

13Librarians Competencies of Library 2.0 Technologies and Service Delivery in Academic Libraries of Akwa Ibom State, Nigeria

Daniel Aniekan Aloysius
Federal Polytechnic, Ukana, Akwa Ibom State
danalo4life@yahoo.com

Eno Torosco Eyene
Akwa Ibom State University, Ikot Akpaden, Akwa Ibom State
enorichard2020@gmail.com

ABSTRACT

Purpose: This study explored librarians' competencies of library 2.0 technologies and service delivery in academic libraries of Akwa Ibom State, Nigeria.
Design: Four research questions and objectives were formulated to guide the study. Survey research design was used in the study. The study population was 63 academic librarians from 11 academic libraries in Akwa Ibom State. All the sixty three academic librarians were sampled. Purposive sampling technique was used in the study. A structured questionnaire was developed and face-validated by the researchers before being used to elicit information from the respondents. All the 63 distributed questionnaires were completed and duly returned. Frequency distribution and percentages were used to analyse the research questions.
Findings: Academic librarians in Akwa Ibom State are aware of the existence of library 2.0 technologies and a significant number of them uses the technology to provide reference, bibliographic, Current Awareness Services (CAS), Selective Dissemination of Information (SDI), advocacy and information literacy services to library clientele.
Practical Implications: The study heightens the need to create more awareness of the existence of the technology to improve library patronage.
Originality/Value: The paper will therefore serve as a prospective reference resource to library management, library and information clientele, researchers and the entire academic community.

Keywords: *Information age, Collaborative learning, Multi-media web-based technologies, Interactive media, Information services*
Paper Type*: Research Paper*

1. Introduction

In the past decades, there has been an exponential growth in the way information are accessed, organized and disseminated due to the emergence of the internet. The internet remains the dominant means of communication in this information age. Statistics from the Internet World Stats (2017) shows that three billion, eight hundred and eighty five people (3,885,000,000), about (51.7%) of the world's population, have access to the internet. The Internet is constantly influencing the development of new modes of scholarly communication; their potential for delivering information is quite vast, as they overcome successfully the geographical limitations associated with the print media. Udofia, Aloysius & Jimmy (2015) described it as the most efficient way to identify, evaluate, retrieve and utilise information in the 21st century information age. Initially, online content was a website-based interface in which only the owner of each individual site had rights to publish information and data, popularly known as Web 1.0 (Handsfield, Dean, & Cielocha, 2009). Presently, information flows through different directions and is more socially inclined, allowing collaborative and interactive forms of learning. The library which is the core of education has been at the lead in application of this technology as it emerged.

Library 2.0 coined by Michael Casey in 2005 from Web 2.0 has helped reposition the library as

the centre for learning and research. Library 2.0 is the application of interactive, collaborative, and multi-media web-based technologies to library services to aid effective use of the library. It uses the web in creation, collection, storage, process, communication and retrieval of information. Mannes (2006) defines Library 2.0 as the application of interactive, collaborative, and multi-media web-based technologies to library services. Kwanya et al. (2011) reiterates that library 2.0 harnesses the power of emerging information and communication technologies to create a dynamic physical and/or virtual library platform which is defined and controlled by the users and librarians and which facilitates the delivery of a superior library experience for the users: anytime and anywhere. Makori (2012) described it as a second generation of web-based services that include social networking sites (such as, Facebook, YouTube, My Space, Flickr, Twitter, and so on) and support systems (like, online help desk) that allows online collaboration, participation, sharing of information and communication services.

Library 2.0 uses the web in creation, collection, storage, process, communication and retrieval. Therefore, library 2.0 can be termed as finding new ways of involving patrons by letting them contribute comments, add tags, rate library items, and get involved in other interactive and collaborative activities of the library. With library 2.0, information and ideas flow in both directions; from the library to the user and from the user to the library. Peltier-Davis (2009) enumerates library 2.0 tools as blogs, wikis, Facebook, twitter, instant messaging, RSS feeds, taggings, podcast Flickr, YouTube, cluster maps, Google page translator, LinkedIn, slide share etc.

For a library user to be able to benefit from the services presented by library 2.0 technology, there is the need for librarians to be able to manipulate the technology efficiently. The inability of librarians to competently use library 2.0 hinders its two-way services thus undermining today's learning system which is user-oriented that allows users to participate in the creation of content. It is pertinent for today's librarians to conveniently use library 2.0 tools to perform virtual reference services, compile bibliographic information and provide other electronic bibliographic services, provide Current Awareness Services (CAS), Selective Dissemination of information services (SDI), information literacy, consortium services and information display and perform advocacy programmes. Librarians can also use library 2.0 tools to organise group discussions with users, market their intellectual contents and perform collegial interactions with staff and students. The ability of librarians to perform these services using library 2.0 tools makes the library a "home" for users and an ideal place for learning.

2. Statement of the Problem

There has been a growing concern of information user's over-reliance on information available at Wikipedia, Google and other social networks. The repercussion of over-reliance on these sources of information is that they are sometimes not verified and authenticated. The web is open for all to display information be it authentic or not. Sometimes, information users seek answers from people on the web with relatively no idea or knowledge of the subject matter. The librarians who are originally the custodians of information are neglected in information search, retrieval and dissemination. This poses grievous effects on the academic and social lives of information users. Several information users complained that they seek help from these categories of persons because academic librarians are in most cases not accessible on the web. Their inaccessibility on the web is attributed to the inability to handle the technology. This raises the concern of the study which is aimed to determine the level of librarian's competencies in the use of library 2.0 technologies.

3. Research Questions

The following research questions were presented to guide the study:

a) Are academic librarians in Akwa Ibom State connected to the internet?
b) Are academic librarians in Akwa Ibom State aware of the existence of library 2.0 technologies?
c) How competent can academic librarians in Akwa Ibom State manipulate library 2.0 technologies?
d) To what extent can academic librarians in Akwa Ibom State use library 2.0 technologies to provide services to

information users?

4. Objectives of the Study

To address the questions, the objectives of the study were:

a) To ascertain if academic librarians of Akwa Ibom State are connected to the internet.
b) To determine the awareness of the existence of library 2.0 technologies by academic librarians in Akwa Ibom State.
c) To establish the extent to which academic librarians of Akwa Ibom State can competently manipulate library 2.0 technologies.
d) To examine the extent to which academic librarians of Akwa Ibom State provides services to information seekers using library 2.0 technologies.

5. Theoretical Foundation and Research Model

The Iceberg Model propounded by McCllelland (1973) contains six competencies: skills, knowledge, social role, self-image, traits and motives. Skills and knowledge are located on the portion of the iceberg that sits above the water level, which is easily seen and relatively easy to determine. Social role, self-image traits and motives are positioned on the iceberg below the water level that is hidden from human eye and are much more difficult to assess than skill and knowledge. The iceberg theory of staff selection is a way of thinking about the characteristics that might make someone a good choice for a particular position in an organisation. The visible part of an iceberg is much smaller than the part that remains hidden underwater.

Similarly, the objective facts about a potential employee are often much important than intangible personal qualities they might bring to the organisation. McCllelland determined that intelligent tests, aptitude tests and personal references were all ineffective ways to determine whether a person would do well in a certain position or not. The author concluded that the factors that allowed some employees to excel were not apparent on the surface, and in some cases were not even known to the employee. Instead of focusing on intelligence or aptitude, McClland focused on competencies.

In the iceberg theory of employee competencies, the skill-set needed for the job is the most obvious competency, followed by knowledge of the job. The employee's own perception of his role in society is less obvious on the surface but a more significant predictor of his success or failure in the position. Still more important yet less apparent are the self-image, personality traits and deepest motives of the employee. When selecting an employee for a job in a company, the iceberg theory advises that employee should not only focus on the visible part of the iceberg but also the hidden part which are looked below the surface of water, and try to determine whether this employee's core competencies would be a good match for the job.

Figure 1: Iceberg Theory of Staff Selection
Source: (Mcllelland D., 1973)

Iceberg theory of staff selection is in correlation with this study based on the fact that skills and knowledge of librarians are essential components in providing effective services to library users. The librarian's ability to manipulate library 2.0 technologies to offer services to information users is more important that having a higher educational qualification. In this case, educational qualification is not a prerequisite for service delivery but the ability to competently use library 2.0 tools to serve the library's teeming patrons is more important.

6. Methodology

6.1 Research Design

Survey design was adopted for this study. Kristonis (2012) defined survey as the collection of data that describes events and then organizes and tabulates the data collection. It is seen as the type of research that studies large and small populations by selecting and studying samples chosen from the population to discover the relative incidence, distribution, and interrelations of sociological and psychological variables. Survey design is used in the study because it facilitates the use of questionnaires with numerically rated items to obtain responses from a target population.

6.2 Area of the Study

The study was conducted in Akwa Ibom state. Created on May 23rd, 1987, Akwa Ibom State is located in the coastal southern part of the country, lying between latitudes 4°32′N and 5°33′N, and longitudes 7°25′E and 8°25′E. It is in the South-South geopolitical zone, and is bordered on the east by Cross River State, on the west by Rivers State and Abia State, and on the south by the Atlantic Ocean and the southernmost tip of Cross River State. Akwa Ibom ranked as the highest oil- and gas-producing state in the country. The states are located on a tropical region, known for heavy rainfall. Major occupations are agriculture, fishing and extraction of raw materials, such as limestone, gold and oil. A sizable number of their population work in the Civil Service Commission. There are approximately 5 million people in the state. The major ethnic groups are Ibibio, Annang and Oron. Several primary, secondary and academic institutions (including the ones under this study) of higher learning are situated in the state.

6.3 Population of the Study

The population of the study is sixty three (63) academic librarians from eleven academic institutions in Akwa Ibom State. The institutions are: University of Uyo, Uyo; Akwa Ibom State University, Mpat Enin; Ritman University, Ikot Ekpene; Akwa Ibom State Polytechnic, Ikot Ekpene; Federal Polytechnic, Essien Udim; Uyo City Polytechnic, Uyo; Maritime Academy, Oron; Heritage Polytechnic, Eket; Sure Foundation Polytechnic, Ukanafun; Akwa Ibom State College of Education, Etinan; and Akwa Ibom State College of Art and Science, Ikono.

Distribution of Population of the Study

S/N	Academic Institutions	Professional Librarians
1.	University of Uyo	27
2.	Akwa Ibom State University	9
3.	Ritman University	1
4.	Akwa Ibom State Polytechnic	3
5.	Federal Polytechnic	7
6.	Uyo City Polytechnic	1
7.	Maritime Academy	5
8.	Heritage Polytechnic	1
9.	Sure Foundation Polytechnic	1
10.	Akwa Ibom State College of Education	7
11.	Akwa Ibom State College of Art and Science	1
	Total	**63**

Source (Office of the Academic Librarians, 2018).

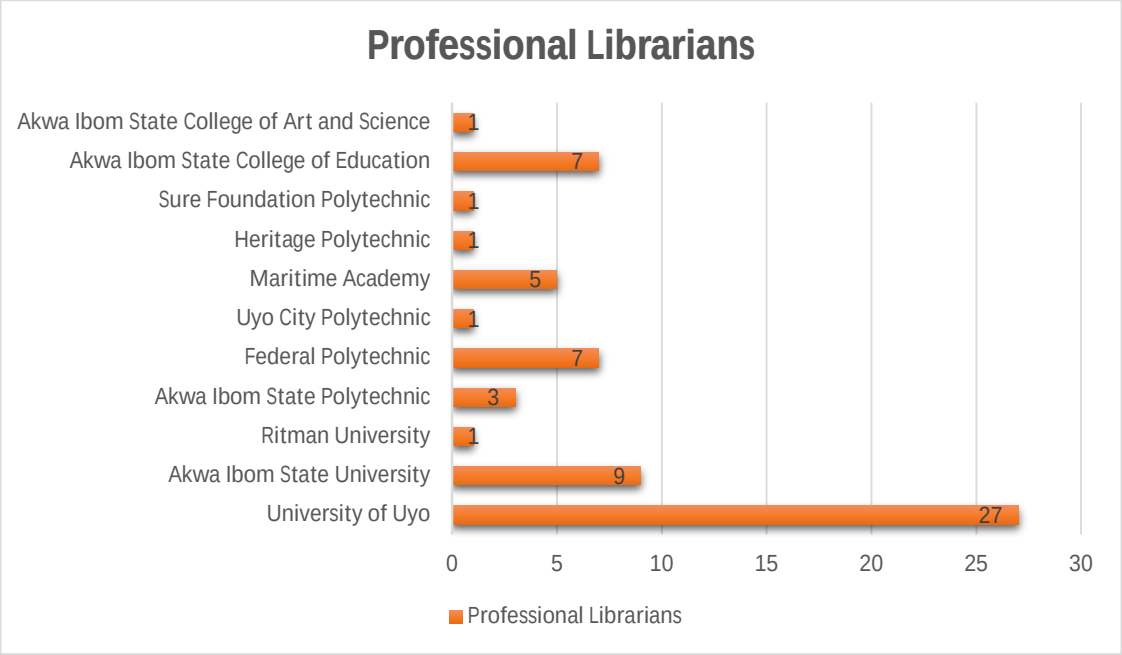


Figure 1: Distribution of Population of the Study

6.4 Sample and Sampling Technique

All the sixty three (63) academic librarians in the eleven academic institutions were sampled. Purposive sampling technique was used in the study.

Sample Frame

S/N	Academic Institutions	Population	Sample
1.	University of Uyo	27	27
2.	Akwa Ibom State University	9	9
3.	Ritman University	1	1
4.	Akwa Ibom State Polytechnic	3	3
5.	Federal Polytechnic	7	7
6.	Uyo City Polytechnic	1	1
7.	Maritime Academy	5	5
8.	Heritage Polytechnic	1	1
9.	Sure Foundation Polytechnic	1	1
10.	Akwa Ibom State College of Education	7	7
11.	Akwa Ibom State College of Art and Science	1	1
	Total	**63**	**63**

6.5 Instrumentation

A structured questionnaire tagged Librarians Competencies in Library 2.0 Technologies and Service Delivery in Academic Libraries Questionnaire (LCLTSDAL) was used to elicit responses from the academic librarians. The instrument contained the questionnaire validated items generated in line with the variables.

6.6 Administration of the Instrument

The questionnaires were administered to the respondents and collected back by the researchers instantly. This ensured 100% return rate of the completed questionnaires, all fully completed as the items were explicitly stated.

6.7 Method of Data Analysis

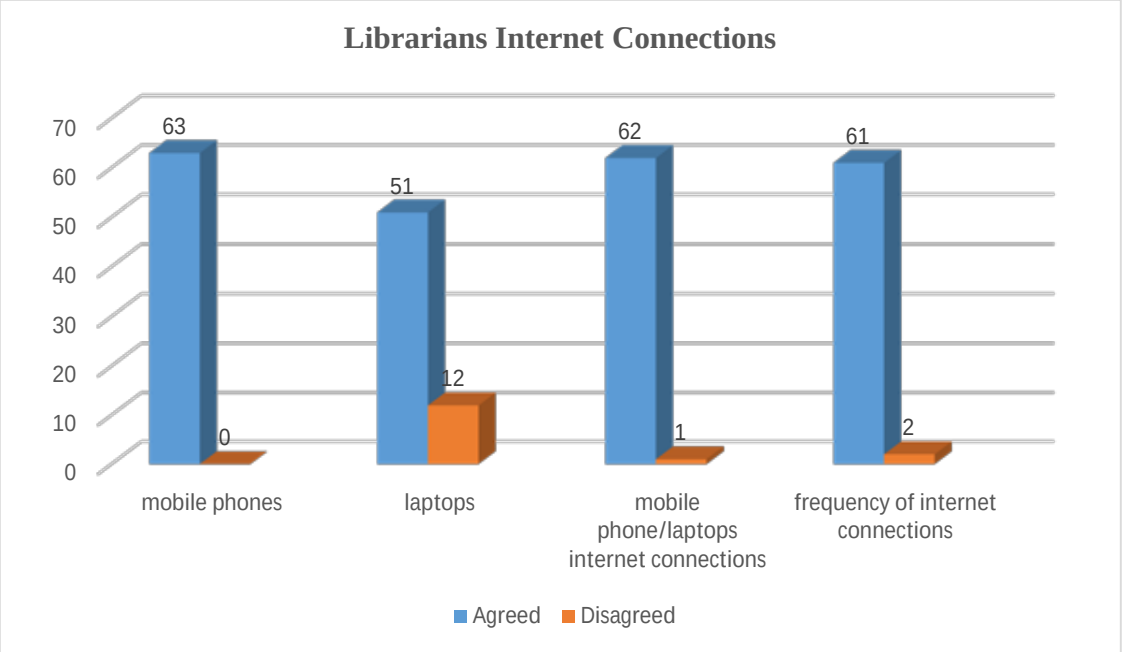
Frequency distribution and percentages were used to analyse the research questions.

7. Results

Frequency Distribution and Percentages of Librarians Competencies of Library 2.0 Technologies and Service Delivery in Academic Libraries are displayed in this section.

Table 3: Librarians Internet Connections of Library 2.0 Technologies

Librarians Internet Connections	SA	A	Total	%	D	SD	Total	%
Do you have a mobile phone?	60	3	63	100	-	-	-	-
Do you have a laptop?	41	10	51	81	5	7	12	19
Is your mobile phone/laptop connected to the internet?	60	2	62	98.4	1	-	1	1.6
How frequent are you connected online?	Daily ☐ 61 (96.8)		Weekly ☐ 1 (1.6)		Monthly ☐ 1 (1.6)		Yearly ☐ -	

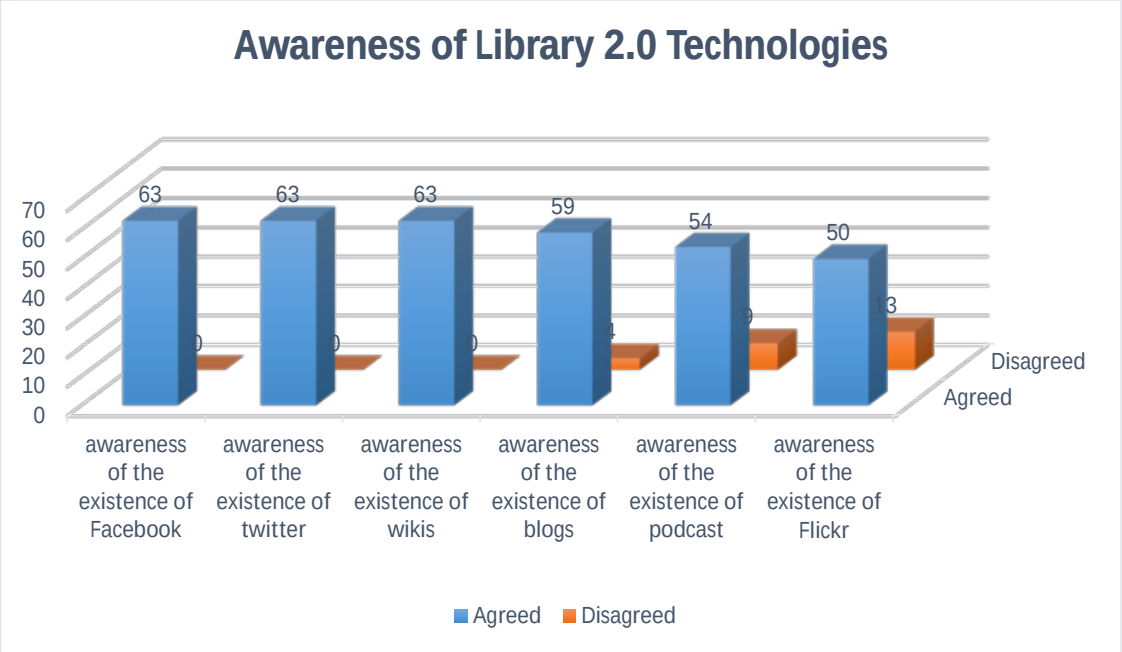


Data obtained in table 3 above indicates that all the professional librarians in academic institutions in Akwa Ibom State have mobile phones. It was revealed further that fifty one (51) librarians have laptops while sixty two (62) of the librarians' mobile phones/laptops are connected to the internet. Data acquired further showed that sixty one (61) librarians access the internet on a daily basis.

Table 4: Librarians Awareness of Library 2.0 Technologies

Awareness of Library 2.0 Technologies	SA	A	Total	%	D	SD	Total	%
Are you aware of the existence of Facebook?	60	3	63	100	-	-	-	-
Are you aware of the existence of twitter?	57	6	63	100	-	-	-	-
Are you aware of the existence of wikis?	52	11	63	100	-	-	-	-
Are you aware of the existence of blog?	50	9	59	93.7	1	3	4	6.3

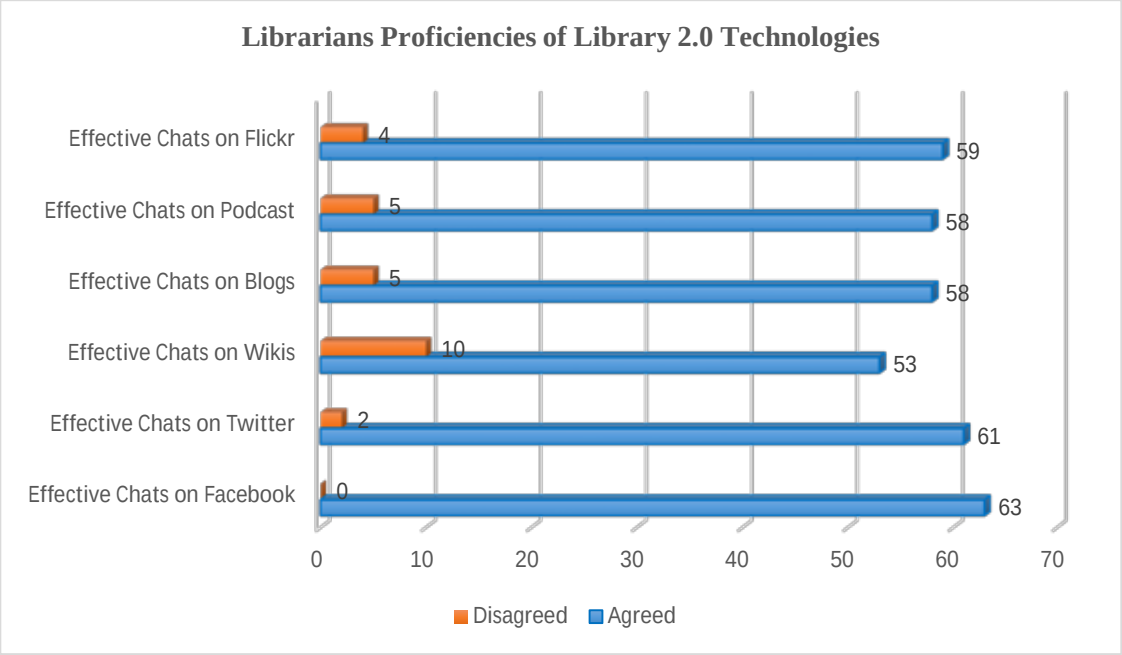
Are you aware of the existence of podcast?	38	16	54	85.7	3	6	9	14.3
Are you aware of the existence of Flickr?	27	23	50	79.4	7	6	13	20.6



In table 4 above, data obtained showed that all the academic librarians are aware of the existence of Facebook, twitter and wikis. Four of the librarians have no knowledge of blogs, nine said they have not heard of podcast while thirteen are not aware of the existence of Flickr.

Table 5: Librarians Proficiencies of Library 2.0 Technologies

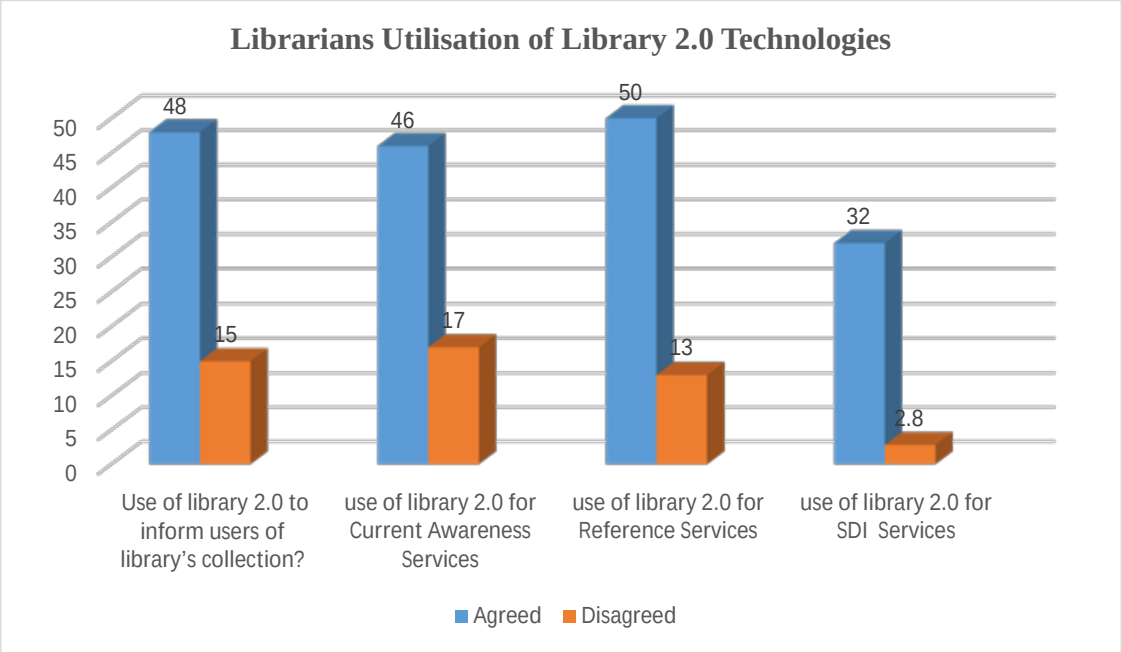
Librarians Proficiencies of Library 2.0 Technologies	**SA**	**A**	**Total**	**%**	**D**	**SD**	**Total**	**%**
Can you effectively chat on Facebook?	51	12	63	100	-	-	-	-
Can you conveniently send and receive messages on twitter?	34	9	61	96.8	1	1	2	3.2
Can you interacts with library patrons on wikis?	35	18	53	84.1	4	6	10	15.9
Can you interact with users through blogs?	27	31	58	92.1	1	4	5	7.9
Can you share audio/video files with users through podcast?	29	21	58	92.1	3	2	5	7.9
You can share photos and graphical documents using Flickr?	30	29	59	93.7	1	3	4	6.3



Data obtained in table 5 above reveals that all the librarians can effectively chat on Facebook. Two of the respondents indicate that they cannot effectively send and receive messages on twitter, ten disagreed on effective use of wikis, five (5) cannot effectively interacts on blogs, five (5) indicate their inability to share audio and video files using podcast while four (4) affirmed that they cannot share graphical documents using Flickr.

Table 6: Librarians' Utilisation of Library 2.0 Technologies for Service Delivery

Utilization of Library 2.0 Technologies for Service Delivery	**SA**	**A**	**Total**	**%**	**D**	**SD**	**Total**	**%**
Have you used any of library 2.0 technologies to inform users of library's collection?	22	26	48	76.2	9	6	15	23.8
Have you provided current awareness services (CAS) through library 2.0 technologies	31	15	46	73	8	9	17	27
Have you answered users query using any of library 2.0 technologies	18	32	50	79.4	4	9	13	20.6
Have you provided Selective Dissemination of Information (SDI) services to users through any of library 2.0 technologies	11	21	32	50.8	20	11	31	49.2



Data obtained in table 6 above reveals that forty eight (48) of the respondents have used library 2.0 technologies to inform users of library's collection, forty six (46) respondents have provided Current Awareness Services (CAS), while fifty (50) respondents have provided reference services to users. Data obtained further shows that thirty two (32) respondents have used library 2.0 technologies to provide Selective Dissemination of Information Services (SDI) to library users.

8. Discussion of Findings

The findings are discussed based on results obtained.

8.1 Academic Librarians Internet Connections

Analysis of the data obtained on internet connections of academic librarians indicated that sixty two (62) librarians out of the sixty three librarians (63) in all academic institutions in Akwa Ibom State have their mobile phones and laptops connected to the internet. As regards the frequency of internet connections, sixty one of the librarians connect to the internet on a daily basis. Only one of the librarians access the internet on a weekly basis and one of them never connects to the internet. The result of this study is in correlation with statistics from the Internet World Stats (2017) that three billion, eight hundred and eighty five million (3,885,000,000) people, about 51.7% of the world's population, have access to the internet.

8.2 Academic Librarians Awareness of Library 2.0 Technologies

Analysis of the data obtained on academic librarians' awareness of library 2.0 technologies indicates that academic librarians in higher institutions in Akwa Ibom State are quite aware of the existence of library 2.0 technologies. Data obtained indicates that all academic librarians are aware of the existence of Facebook, three are not aware of the existence of blogs, nine (9) are not aware of podcast and thirteen not aware of the existence of podcast.

8.3 Academic Librarians Proficiencies in use of Library 2.0 Technologies

Analysis of the data obtained on academic librarian's proficiencies in their use of library 2.0 technologies shows that academic librarians in academic institutions in Akwa Ibom State can competently use library 2.0 technologies. All the librarians sampled indicates that they can conveniently chat on Facebook while sixty one (61) librarians stated that they can send and receive messages on twitter. Data obtained further reveals

that majority of the librarians can interacts with library users on wikis, blogs and they can also send and receive audio, video, photos and graphical documents on podcast and Flickr.

8.4 Academic Librarians Utilisation of Library 2.0 Technologies

Analysis of the data obtained on academic librarians' utilisation of library 2.0 technologies reveals that a significant number of librarians use library 2.0 technologies for service delivery to library users. Data obtained shows that forty eight librarians have used library 2.0 technologies to inform users of library collection, forty six librarians have used it for current awareness services, fifty (50) and thirty two (32) librarians have used it for reference and Selective Dissemination of Information services, respectively.

9. Conclusion

The application and utilization of library 2.0 technologies in library services in this information age cannot be over-stressed. Library services have transmuted from physical and passive to virtual and collaborative. Academic librarians in higher institutions in Akwa Ibom State are well conversant with library 2.0 technologies. The study evidently showed that academic librarians use the technologies in to provide reference, bibliographic, Current Awareness, Selective Dissemination of Information and information literacy services. Librarians also uses the technologies for advocacy outreaches. However there is the need for some of the librarians who opined ignorance of some of the library 2.0 technologies to keep abreast with the existing technologies to enhance effective service delivery to information users.

10. Recommendations

Based on the findings, the paper therefore concludes that management of academic libraries should organise advocacy programmes to inform librarians and information users on the existence and utilization of other library 2.0 technologies. The organization of these programmes will invariably create more awareness of the existence of the technology and improve library patronage. Platforms such as "Library Discussion Group" should be created by academic librarians to provide library services such as Current Awareness Services (CAS), Selective Dissemination of Information (SDI), reference and bibliographic services. Apparently, the provision of this service will offer varied access to current and reliable information for learning and research. Library management are requested to organise special training and re-training programmes for librarians and other library staff to enable them effectively manipulate the technologies. The ability of academic librarians to be able to handle library 2.0 technologies will aid effective service delivery. More importantly, management of academic libraries in Nigeria and Akwa Ibom State in particular should equip their libraries with adequate computers and other Information and Communication Technologies to enhance effective access and retrieval of information resources.

References

Handsfield, L. J., Dean, T. R., & Cielocha, K. M. (2009). Becoming critical consumers and producers of text: Teaching literacy with Web 1.0 and Web 2.0. *Reading Teacher*, *63*(1), 40-50.

Internet World Stats (2017). Today's road to e-commerce and global trade internet technology reports. Retrieved from Internet%20Growth%20Statistics%201995%20to%202017%20-%20the%20Global%20Village%20Online.htm.

Kristonis, W. A. (2012). Research design and methods. Retrieved from: http://www.slideshow.net

Kwanya, T., Stilwell, C., & Underwood, P. G. (2011). Library 2.0: Revolution or evolution? *South African Journal of Libraries & Information Science*, 75(1), 70-75.

Makori, E. O. (2012). Potential of library 2.0 in provision of information services in academic libraries. Paper presented at SCESAL XXth Conference hosted by KLA on 4th-8th June Laico Regency Hotel, Nairobi, Kenya. Retrieved from scesal.viel.co.ke/images/c/ce/POTENTIAL.

Mannes, J. M. (2006). Library 2.0 theory: Web 2.0 and its implications for libraries. *Webology* 3

(2), 25. Retrieved from http://www.webology.org/2006/v3n2/a25.html.

Mclleland, D. (1973). The iceberg theory of staff selection/business and entrepreneurship. Retrieved from: yourbusiness.azcentral.com>.

Peltier-Davis, C. (2009). Web 2.0, library 2.0, library user 2.0, librarian 2.0: Innovative services for sustainable libraries. *Computers in Libraries*, 29 (10), 16-21.

Udofia, Aloysius & Jimmy (2017). Internet resources and information literacy of hearing and speech impaired students in Nigerian academic libraries. *Computing and Information Systems Journal*, 21 (1), 18-31.

Appendix A

Questionnaire on Librarians Competencies of Library 2.0 Technologies and Service Delivery in Academic Libraries of Akwa Ibom State

S/N	Librarians Internet Connection	Strongly Agree	Agree	Disagree	Strongly disagree
1	Do you have a mobile phone?				
2	Do you have a laptop?				
3	Is your mobile phone/laptop connected to the internet?				
4	How frequent are you connected online?	Daily ☐ Weekly ☐ Monthly ☐ arly ☐			
	Awareness of Library 2.0 Technologies				
5	Are you aware of the existence of Facebook?				
6	Are you aware of the existence of twitter?				
7	Are you aware of the existence of wikis?				
8	Are you aware of the existence of blog?				
9	Are you aware of the existence of podcast?				
10	Are you aware of the existence of Flickr?				
	Librarians Manipulative Skills				
11	Can you chat effectively on Facebook?				
12	Can you conveniently send and receive messages through twitter?				
13	Can you interact with library patrons on wikis?				
14	Can you interact with users through blogs?				
15	Can you share audio/video files with users through podcast?				
16	You can share photos and graphical documents using Flickr?				
	Utilization of Library 2.0 Technologies for Service Delivery				
17	Have you used any of library 2.0 technologies to inform users of library's collection?				
18	Have you provided current awareness services (CAS) through library 2.0 technologies				
19	Have you answered users query using any of library 2.0 technologies				

20	Have you provided Selective Dissemination of Information (SDI) services to users through any of library 2.0 technologies				

About the Authors

Mr. Aloysius, Daniel Aniekan is a Chartered Librarian of Nigeria (CLN) and a Doctoral student in the Department of Library and Information Science, University of Uyo, Akwa Ibom State, Nigeria. He specialises in Information Technology and has articles in reputable local and foreign journals. Mr. Aloysius, Daniel Aniekan is the Head of Electronic Unit, Federal Polytechnic Library, Ukana, Akwa Ibom State, Nigeria. Email: danalo4life@yahoo.com.

Mrs. Eno Torosco Eyene is a Chartered Librarian of Nigeria (CLN) and holds a Master's Degree in Library and Information Science from the University of Calabar, Cross River State. She is presently an Assistant Librarian and Head of Readers Services of the Akwa Ibom State University library, Ikot Akpaden, Mpat Enin L.G.A, Akwa Ibom State, Nigeria. Mrs. Eno Torosco Eyene has published several articles in reputable journals. Her email is enorichard2020@gmail.com

Effectiveness of Contraceptive Usage among Reproductive Ages in Nigeria Using Artificial Neural Network (ANN)

[1]Kazeem A. Dauda, [2]Akinbowale N. Babatunde, [3]Kabir O. Olorede, [4]Sulaiman O. Abdulsalam and [5]Oluwaseun R. Ogundokun

[1,3]Department of Statistics and Mathematical Sciences, Kwara State University, Malete, P.M.B 1530, Ilorin, Nigeria.
kazeem.dauda@kwasu.edu.ng and kabir.opeyemi@kwasu.edu.ng

[2,4]Department of Computer Sciences, Kwara State University, Malete, P.M.B 1530, Ilorin, Nigeria.
akinbowale.babatunde@kwasu.edu.ng and sulaiman.abdulsalam@kwasu.edu.ng

[5]Department of Computer Science, Landmark University, Omu-Aran, P.M.B 1001, Omu-Aran, Nigeria.
ogundokun.roseline@imu.edu.ng

ABSTRACT

Purpose: Contraceptive usage among women of reproductive age is a fertile area of research for the medical scientists, social scientists, and medical practitioners. However, not much work has been done in Nigeria to identify some of the contraceptive methods used in preventing unwanted pregnancy and sexually transmitted infection (STI) diseases, particularly to explicitly determine which of them are most effective. This paper tackles this task.

Methodology: In this paper, we examine different types of contraceptive methods used by Nigeria women to prevent unwanted pregnancy. Datasets on contraceptive usage among 28,647 women of reproductive age from the 2008 Nigerian Demographic Health Survey (NDHS) were analyzed using Artificial Neural Network (ANN) approach in the R language.

Finding/Results: The results of the analysis revealed that approximately 1%, 3% and 9% of the study population were using Folkloric, Traditional and Modern methods, respectively. Additionally, 12%, 3% and 9% of the women were found to be currently using the methods since last birth and before last birth. Furthermore, the ANN results through the Garson algorithm revealed that using the modern methods (IUD, Norplant and Female condom) and the traditional methods prevents the unwanted pregnancy negatively, while other modern methods (pill, male condom, female sterilizer, periodic abstinence, withdrawal, locational amenorrhea and foam or jelly) were found to be effective in preventing unwanted pregnancy positively. Interestingly, women that used the modern methods (i.e. Pill, IUD, Injection, Male condom, Female sterilization, Periodic abstinence, Withdrawal and Lactational amenorrhea) were found to be effective in preventing unwanted pregnancy.

Research Limitation: The main limitation of this study is the inability to access the current data from NDHS. Therefore, the conclusion of this study is only based on the 2008 NDHS data.

Originality/Value: This research work introduces artificial neural network (ANN) to determine and identify the effect of contraceptive methods usage among Nigeria women, and to determine their level of important using Garson's algorithm variable important. This introduction measures the nonlinear effect that exists between the methods and response variable (pregnant and no pregnant) which existing research approaches do not.

Keywords*: Contraceptive methods, Variable Important, Garson Algorithm, Artificial Neural Network (ANN) and Data mining.*

[1]Corresponding Author: alt. email: qdauda@yahoo.com/qdauda70@gmail.com

1 Introduction

Contraception is defined as the prevention of conception without abstinence (Ladipo and Akinso, 2005). There are traditional methods of contraception, which include withdrawal and rhythm, and there are modern contraceptive methods, which include the hormonal and non-hormonal methods. The hormonal methods include oral pills, injectable and subdermal implants and some intrauterine contraceptive devices whereas non-hormonal contraceptives include condoms, intrauterine devices like Copper-T and sterilization (Tubal Ligation in women and vasectomy in men (Hatcher et al., 1997). For most methods, effectiveness depends on user compliance, which may be improved by information provision, counseling and the support of health care providers. For some

methods, efficacy also depends on aspects of healthcare provision.

1.1 The risk of pregnancy versus the risk of the method

The relative risks associated with the use of a particular contraceptive need to be balanced against the risks of pregnancy.

When a woman has a condition that makes unplanned pregnancy an unacceptable health risk, the sole use of methods with a relatively high typical use failure rate, including barrier methods and Fertility Awareness-Based Methods (FABMs) may not be appropriate (Cavazos-Rehg et al., 2015). Some of these conditions include recent breast cancer, complicated valvular heart disease, ischaemic heart disease (IHD) or stroke, malignant gestational trophoblastic disease and malignant liver tumors severe (decompensated) cirrhosis.

1.2 Effectiveness

The average pregnancy rate, when no contraception is being used, is approximately 20% per cycle, with rates depending on the age of the couple and frequency of sexual intercourse. The effectiveness of a contraceptive method is most easily defined as the number of unintended pregnancies occurring in a year for every 100 women using the method. For example, if a method has an effectiveness of 99% this can be explained as either: 99 women out of 100 women using the method in a year being protected against an unintended pregnancy or 1 woman out of every 100 women using the method becoming pregnant in a year.

The effectiveness of the method for an individual woman will depend on the inherent method characteristics, the woman's own fertility status and her adherence to the method, e.g. the ability to remember a daily contraceptive pill or the ability to correctly use a male or female condom. Contraceptive effectiveness is also described by the Pearl Index, which is derived by dividing the number of unintended pregnancies occurring with a method, by the number of years of exposure to the risk of unintended pregnancy during a study (Bradshaw and Brook, 2014).

1.3 Worldwide Contraceptive Prevalence

Worldwide contraceptive prevalence (the percentage of married women currently using contraception) was estimated to be 58% in, with contraceptive use in the developed regions at 70% and in the developing regions at 55% (WHO, CCP, USAID, 2011). Among the developing areas, contraceptive prevalence is lowest in Africa where on average only one out of five married couples is currently using a contraceptive (WHO, 2015). In Asia and Latin America and the Caribbean, contraceptive use is similar. However, data at the regional levels reveal greater divergence than is implied by the overall averages (WHO, CCP, USAID, 2011**).**

Monjok et al. (2010) estimated that of the 210 million pregnancies that occur annually worldwide, about 80 million (38%) are unplanned and 46 million (22%) end in abortion. More than 200 million women in developing countries would like to delay their next pregnancy or even stop bearing children altogether (Diaz, 2002), but many of them still rely on traditional and less effective methods of contraception or use no method at all. Those who do not use any contraceptive method may lack access or face barriers to using contraception (Diaz, 2002). These barriers include lack of awareness, lack of access, cultural factors, religion, opposition to use by partners or family members, and fear of health risks and side effects of contraceptives (DeRose et al., 2004).

In many developing countries (also termed low- and middle-income countries), official family planning programmes began during the 1960s with the aim of reducing high fertility i.e. high numbers of births per woman (Diaz, 2002). However, in recent years, various Demographic and Health Surveys (DHS) report that women in developing countries have lower desired fertility than actual fertility, i.e. women are having more children than they want. This indicates that there is still an unmet need for family planning i.e. there is the proportion of women of reproductive age who prefer to avoid or postpone childbearing but who are not using any method of contraception. In 2000, an estimated 17% of married women (105 million) had an unmet need for family planning in the developing world (USAID, 2013), and there is considerable variation across countries, for example, 5% in Vietnam and 40% in Haiti.

1.4 Nigeria Contraceptive Prevalence Perspective

In Nigeria, unintended intercourse is the primary cause of unwanted pregnancies, and many women with unwanted pregnancies decide to end them by abortion (Otoide et al., 2001). Since abortion is illegal in Nigeria (unless medically recommended to save a mother's life) many abortions are carried out in an unsafe environment (Abiodun and Balogun, 2009). The consequences of these clandestine abortions are grave and can be life-threatening, often leading to maternal death. Abortions account for 20% to 40% of maternal deaths in Nigeria (Oriji et al., 2009).

Many Nigerian women of reproductive age experience unwanted pregnancies and resort to abortion (Otoide et al., 2001). According to a DHS survey of women in southwestern and northern Nigeria, at least 20% reported having experienced an unwanted pregnancy (Nigeria Demographic and Health Survey, 2008). The 2008 DHS found that of the total live births reported in the three years prior to 2008, 15% were also reported to be unplanned.

Contraception has been identified as an effective means of combating the problem of unwanted pregnancy and unsafe abortion. It is equally an effective means of family planning and fertility control and therefore very important in promoting maternal and child health. Access to quality reproductive health and family planning services remain poor in Nigeria (Abiodun and Balogun, 2009).

1.5 Choice of contraceptive methods

Four pieces of information about contraceptive efficacy would help couples to make an informed decision when choosing a contraceptive method: Pregnancy rates during typical use show how effective the different methods are during actual use (including inconsistent or incorrect use). Secondly, pregnancy rates during perfect use show how effective methods can be, where perfect use is defined as following the directions for use.

Thirdly, pregnancy rates during imperfect use show how ineffective methods would be if they are used incorrectly or inconsistently. Pregnancy rates can be computed separately for different categories of imperfect use to reveal which types of imperfect use are most risky. Lastly, the percentage of perfect users or percentage of months during which a method is used perfectly reveals how hard it is to use a method correctly and consistently.

1.6 Data Mining

The process of discovering interesting knowledge, which includes patterns, associations, changes and significant structures from a large amount of data set from statistical perceptive is regarded as *Data Mining* (Fayyad, 1996). It is also seen as nontrivial extraction of implicit, previously unknown, and potentially useful information from data using machine learning, statistical and visualization techniques (Frawley, 1991). Data mining has proved to be valuable in numerous application, due to increase in technology around the globe (Vapnik, 1998; Hastie et al., 2001; Witten and Frank, 2005; Felici and Vercellis, 2007). The majority of the problems studied in the data mining community can be categorized as Decision Trees, Neural Networks, Rule Induction, Nearest Neighbors, and Genetic Algorithms (Hastie et al., 2001).

Data mining is noted for its pattern recognition ability that ensures that information is obtained from vague data. In particular, unique or valuable relationships between and within the data can be identified and used proactively to categorize or anticipate additional data. Through the use of exploratory graphics in combination with advanced statistics, machine learning tools, and artificial intelligence, critical "nuggets" of information can be mined from large repositories of data.

Many techniques have been developed for data mining and the methods for analyzing and modeling data can be divided into two groups: supervised learning and unsupervised learning. Supervised learning requires input data that has both predictor (independent) variables and a target (dependent) variable whose value is to be estimated. By various means, the process learns how to model (predict) the value of the target variable based on the predictor variables. Unsupervised learning does not identify a target (dependent) variable but rather treats all of the variables equally. In this case, the goal is not to predict the value of a variable but rather to look for patterns, groupings or other ways to characterize the data that may lead to an understanding of the way the data interrelates.

Data mining can be used to generate a hypothesis and it uses modeling techniques. In the past, data mining processes were summarized as a collection of statistical analysis. However, the addition of machine learning and intelligent processes such as Artificial Neural Networks, Genetic Algorithms, Fuzzy Logic,

and modified cluster analyses have considerably increased the capabilities and utilities offered by data mining. Data mining uses machine learning, statistical and visualization techniques to discover and present knowledge in a form that is easily comprehensible to humans. The most common data mining tasks are based on classification, clustering, and discovery of association rules. Others include prediction, characterization, deviation analysis and outlier analysis. Data mining is more oriented towards applications than the basic nature of the underlying phenomena. It is relatively less concerned with identifying the specific relations between the involved variables. Instead, the focus is on producing a solution that can generate useful predictions. Therefore, data mining accepts among others a "black box" approach to data exploration or knowledge discovery (Felici and Vercellis, 2007).

In this work, we apply Artificial Neural Networks (ANN) to NDHS survey data conducted in 2008.

1.6.1 Artificial Neural Network (ANN)

An Artificial Neural Network (ANN) is a mathematical model that tries to simulate the structure and functionalities of biological neural networks. The basic building block of every artificial neural network is an artificial neuron, that is, a simple mathematical model (function). Such a model has three simple sets of rules: multiplication, summation, and activation. Every input is weighted which means that every input value is multiplied by individual weight at the initial state of Artificial Neuron. The sum function that adds up all weighted inputs and biases of Artificial Neuron occur in the middle section. At the final state of artificial neuron, the previously sum weighted inputs and bias are passing via activation function that is also called transfer function (Figure 1.) (Andrej et al., 2011).

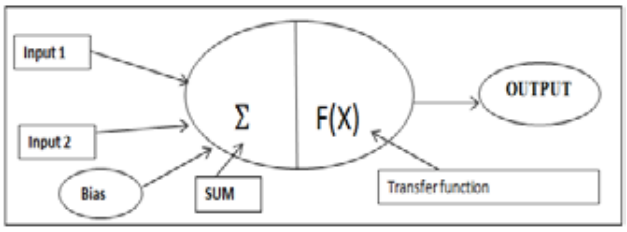


Figure 1: Artificial Neuron Design

2 Methodology

The data used for this research was obtained from the Nigerian Demographic and Health Survey (NDHS), and it covers 28,647 women of reproductive age (respondents), throughout the nation. The minimum and maximum ages of the respondents are 13 years and 45 years, respectively. Yahya et al. (2012) used a similar age range.

The response variable is pregnant status, which is categorized into distinct groups. The first group is those that answered “Yes” and the second group is those that answered “No”. This makes it a dichotomous response variable. The scale of 0 for the category "No" and 1 if another category that is "Yes".

Apart from the Response variable, the categorical variables were also involved and regarded as independent variables. These are currently used, used since, used before, using modern, using traditional, pill, IUD, injection, condom, female sterilizer, periodic, withdrawal, other, Norplant, lactation, female condom, and form or jelly.

The original function of neural network (NN) was the computer-based model used to mimic the human brain. The most widely used NN is called the Multi-layer perceptron (MLP) system, which consists of a set of input features, a number of interactive layers, in between the inputs and output layers and specifically one output layer (Yahya et al, 2012). The simplest multilayered perceptron is given in the equation below

$$o(x) = f(w_0 + \sum_{i=1}^{n} w_i x_i) \quad (1)$$

Where w_0 denotes the intercept, $w_i = (w_1, w_2, \dots, w_n)$ the vectors consisting of all synaptic weight without the intercept, and $x = (x_1, x_2, \dots, x_n)$ the vector of all independents variable (Frauk and Steven, 2010). Since the response variable is binary, sigmoid function (transfer function) is suitable for our ANN construction.

After experimenting with the equation (1) on the real-life data set discussed earlier, the contribution of the independent (contraceptive methods) variables on the response variable was measured using Garson Algorithm (1991) technique. The algorithm partitions the hidden layer weights into components associated with each input node. Subsequently, the percentage of all hidden node weight associated with the input node was used to measure the relative importance of that attribute. In general, for each input j, where

$j = 1,2,\ldots,i$, the relative importance (RI_j) can be calculated using the equation (2).

$$RI_j = \frac{\sum_{m=1}^{N_h}\left[\left[\frac{|w_{jm}^{ih}|}{\sum_{k=1}^{N_i}|w_{km}^{ih}|}\right]\times|w_{jm}^{ho}|\right]}{\sum_{n=1}^{N_i}\left[\sum_{m=1}^{N_h}\left[\left[\frac{|w_{nm}^{ih}|}{\sum_{k=1}^{N_i}|w_{km}^{ih}|}\right]\times|w_{jm}^{ho}|\right]\right]} \quad (2)$$

In equation (5), N_i and N_h are the numbers of inputs and hidden neurons respectively, w is the connection weight, the superscripts $"i","h"\ and\ "o"$ refer to input, hidden and output layers, respectively and subscripts $"k","m"\ and\ "n"$ refer to input, hidden and input neurons used. In our case, there is only one output neuron. In this algorithm, each input node j, the relative contribution of j to the outgoing signal of each hidden neuron, is calculated and presented in percentage, which then serves as a measure of importance for each node of the given variable. Additionally, the entire input variables with the smallest contribution to the final output of the network are eliminated (Garson Algorithm., 1991).

3 Experimental Results

Table 1 describes the dataset using simple percentages.

Table 1: Description of the dataset using simple percentages

Determinants	**Factor levels**	**Currently Pregnant**		**Total 28,647 (100%)**
		No (0) 24,953 (87.1%)	Yes (1) 3,694 (12.9%)	
Current methods used	No method	21,258 (85.2%)	3,694 (14.8%)	24,952 (87.1%)
	Folkloric method	187 (100%)	0 (0.0%)	187 (0.65%)
	Traditional method	885 (100%)	0 (0.0%)	885 (3.09%)
	Modern method	2,623 (100%)	0 (0.0%)	2,623 (9.16%)
Pattern of use	Currently using	3,695 (100%)	0 (0.0%)	3,695 (12.9)
	Used since last birth	473 (50.4%)	466 (49.6%)	939 (3.28)
	Used before last birth	2,309 (86.2%)	370 (13.8%)	2,679 (9.35)
	Never used	18,476 (86.6%)	2,858 (13.4%)	21,334 (74.47%)

However, for the currently used methods, the analyses show that out of the 24,952 respondents that used "No method", 3,694 (14.8%) have the chance of having a pregnancy of which 21,258 (85.2%) are pregnant free. Also for the “folkloric method”, out of 187 women who practice this method none of them had a pregnancy. Likewise for “Traditional method”, 885 women who practiced this method were pregnant free. So also for the “Modern method”, 2,623 women who practice this method are also pregnant free (i.e. Folkloric, Traditional and modern method are very efficient).

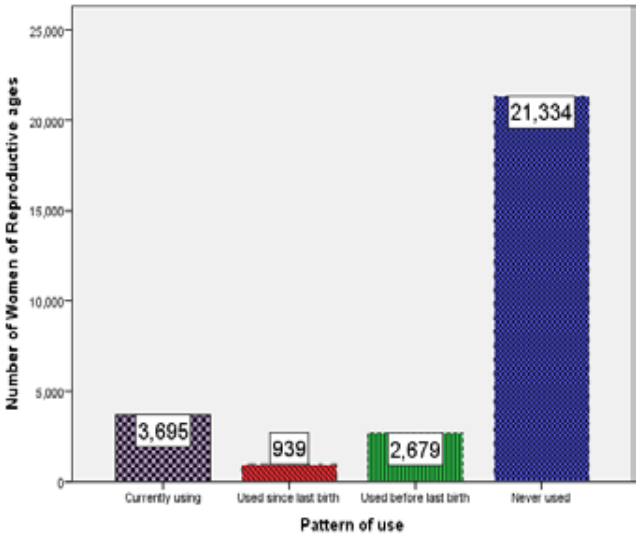


Figure 2: Virtual display of the pattern of use

Furthermore, the pattern of use for those that are currently using the method (contraceptive method) shows that 3,695 women currently practicing (contraceptive methods) are pregnant free. Out of 939 women who used since last birth 466 (49.6%) have pregnancy and 473 (50.4%) are pregnant free, also out of 2,679 who used before last birth, 370 (13.8%) were pregnant and 2,309 (86.2%) were free from having pregnant, and out of 21,334 women that never used any means of contraceptive methods, 2,858 (13.4%) have pregnancy and 18,476 (86.6%) are pregnant free.

Figure 2 shows the virtual display of the pattern of contraceptive usage among women. It was observed that "Never used" (contraceptive method) has the highest number of reproductive ages with a total of 21,334 and number of reproductive ages that has the lowest pattern of use is the "Used since last birth" with total of 939, while currently using and used before last birth has number of reproductive ages of totals 3,695 and 2,679 respectively.

Table 2: Variable Important by Garson Algorithm

Covariate	**Relative important**	**Remarks on the pregnancy status**
Currently, use	-0.3544	Weak Negative relationship
Used since	1.0000	Strongest Positive relationship
Used before	0.0000	No substantial importance
Using modern	-0.0723	Very weak Negative relationship
Using traditional	-0.1449	Very weak Negative relationship
Pill	0.4690	Strongest Positive relationship
IUD	-0.1543	Very weak Negative relationship
Injection	0.0809	Very weak Positive relationship
Condom	0.2099	Strongest Positive relationship
Female sterilizer	0.0614	Very weak Positive relationship
Periodic	0.2329	Strongest Positive relationship
Withdrawal	0.2084	Strongest Positive relationship
Other	0.1318	Very weak Positive relationship
Norplant	-0.1479	Very weak Negative relationship
Lactation	0.1186	Very weak Positive relationship
Female condom	-0.1014	Very weak Negative relationship
Foam or Jelly	0.0900	Very weak Positive relationship

The Table 2 above shows that "Currently used" which is among the pattern of use method by the women of reproductive ages has a weak negative relationship to the response variable. This implies that women who "Currently used" contraceptive methods have -0.3544 association towards the pregnant status. While "Used since" which indicates a pattern of contraceptive usage among women since last birth has the strongest positive relationship to the response variable. This also implies that women who make use of the "used since" method have 100% correlation towards the pregnant status. Moreover, "Used before" which indicates a pattern of a used method before the last birth has no relationship to the response variable and implies that women who practice "used before" method have 0% association towards the pregnant status.

Nevertheless, “Using modern and traditional methods” which indicate the current methods used by the women has a weak negative relationship to the response variable and implies that women who are “using modern and traditional” methods have -0.0723 and -0.1449 associations towards the pregnant status. The Pill, Condom, Periodic and Withdrawal among the contraceptive methods have strong positive relationships to the response variable. This implies that women who use these methods have 0.4690, 0.2099, 0.2329 and 0.2084 correlation towards the pregnant status.

Finally, other contraceptive methods which include "Injection, Female sterilizer, Other, Lactation, and Foam or Jelly, IUD, Norplant, and Female condom” suffer from a very weak positive and negative relationship with the response variable. These also imply that women who practice these methods have weak degrees of association towards the pregnant status.

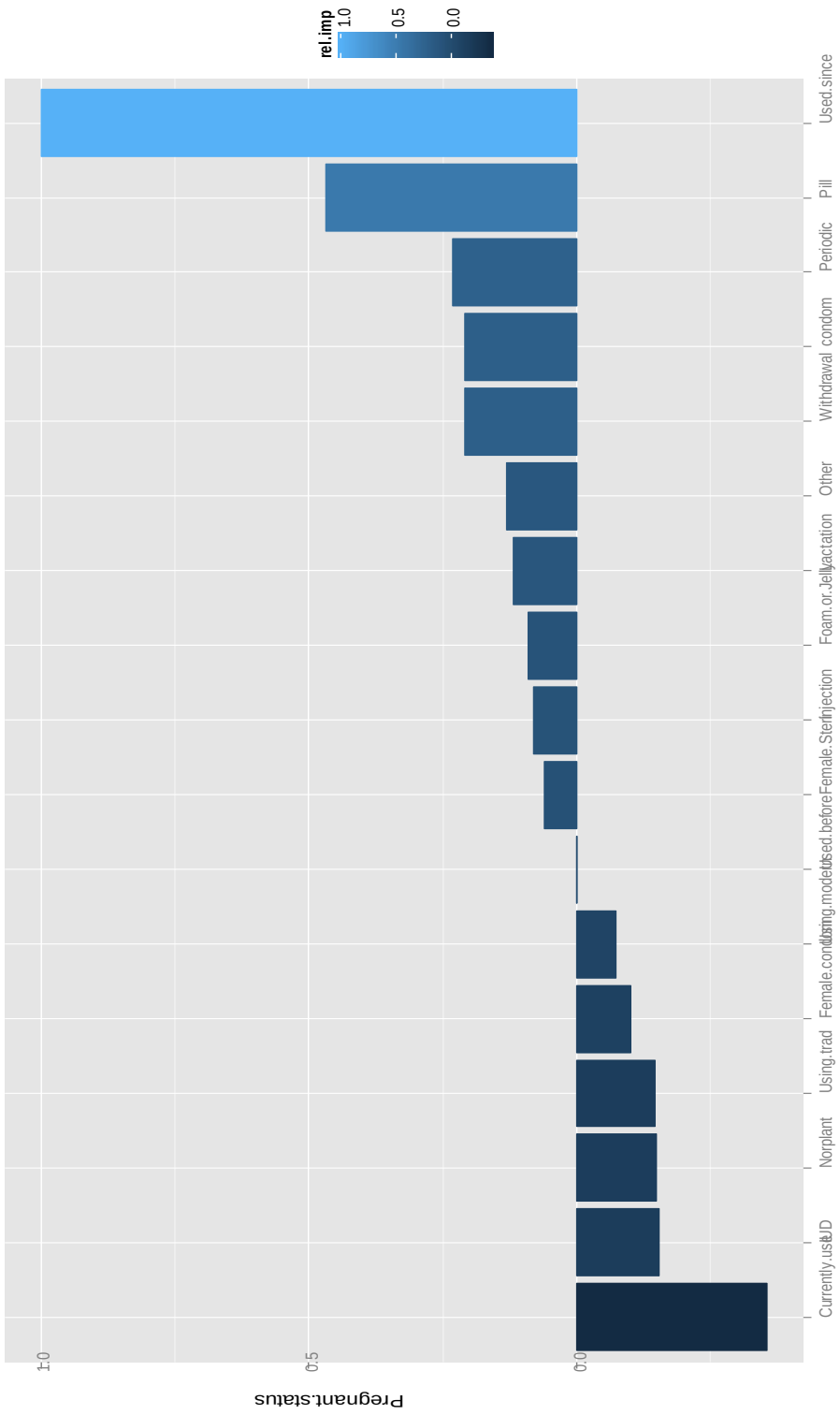


Figure 3: Relative important of the seventeen contraceptive methods against the response (pregnant status) variable

The relative important value in Table 2 and Figure 3 was determined using the method of Garson (1991). The results tell us that the covariates "used since" have the highest relative importance. Pill, condom, periodic and withdrawal methods have the strongest positive relationship, individually with the response (pregnant status). Correspondingly, covariates that have relative important to be zero such as the "used before" method do not have any substantial importance for response variable. Nevertheless, this covariate with zero relative importance most likely has some marginal effect on the response variable, but its effect is irrelevant in the context of the other covariates. Other covariates were found to have either very weak positive or negative relationships with the response variable as shown in Table 2.

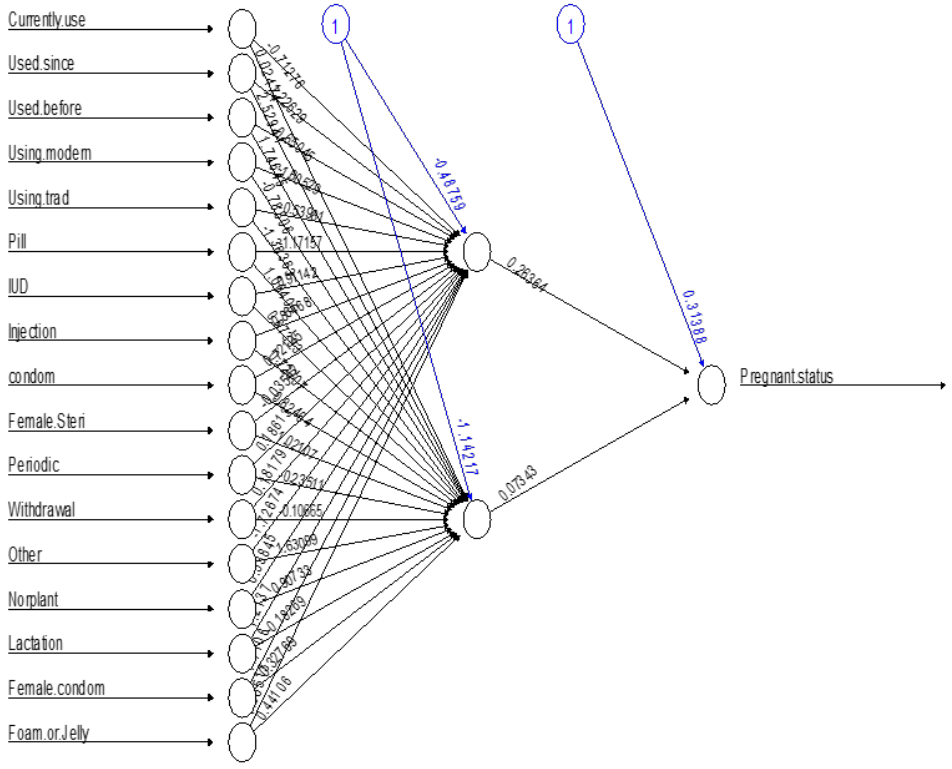


Figure 4: Plot of a trained neural network including trained synaptic weights and basic information about the training process.

Here, we present the virtualization of the results of the training process of MLP model with 2 hidden layers as shown in Figure 4. The plot includes the trained synaptic weights, different intercept and basic information about the training process such as the overall error and number of steps which produce one response (pregnant status).

4 Discussion of Results

Various facility factors were considered, among which are the quality of family planning services. This study was conducted with the aim of examining the effectiveness of contraceptive usage among women of reproductive age in Nigeria, because several contraceptive methods have been put in place, and all claim to be effective in preventing unwanted pregnancy and STI. Based on the NDHS 2008 survey, contraceptive methods are classified as modern or traditional methods. Modern methods include female sterilization, the pill, intra-uterine device (IUD), injectables, implants, female condom, foam/jelly, lactational amenorrhea method (LAM), and emergency contraception. Methods such as periodic abstinence and withdrawal are grouped as traditional methods. Women of reproductive ages in Nigeria who

practice contraceptive methods have the total of 28,647 respondents, and 3,694 have the chance of getting pregnant, and this shows that some methods are not effective as claimed. Nevertheless, 87.1% are those who are not practicing any form of contraceptive methods and the main reason for non-usage of contraceptive methods was fear of side effects and the desire to have more children.

Lastly, we proceed to the artificial neural network (ANN) through the use of "Neuralnet" package in R to identify some important variables (contraceptive methods) using Garson algorithm (1991). The results reveal the relative importance of the seventeen covariates (contraceptive methods) and we observed that "used since" (i.e., women that has been using the contraceptive method for a long time) has the strongest positive relationship with the pregnant status follow by "currently used" (i.e., women that are just using the contraceptive method) with a weak negative relationship. Finally, "used before" (i.e., women that stopped using contraceptive method) has no any substantial relationship with pregnant status.

5 Conclusions

This study has been useful in identifying some of the contraceptive methods that are effective in preventing unwanted pregnancy and sexually transmitted infection (STI) among women of reproductive ages in Nigeria and the findings should help in monitoring the reproductive status of the family. However, there was also a large portion of those who were not using contraceptive methods and this can increase the population of a country. Different types of birth control methods have large differences in effectiveness, action required of users, and side effects. Thus, different methods require different actions of users.

References

Abiodun, O. M., & Balogun O. R. (2009). Sexual activity and contraceptive use among young female students of tertiary educational institution in Ilorin, Nigeria. *Contraception*, Vol. 79, pp. 146–149. http://dx.doi.org/10.1016/j.contraception.2008.08.002

Adesiyun, A. G. (2007) Female sterilization by tubal ligation: A re-appraisal of factors influencing decision making in a tropical setting. *Arch Gynecol Obstet*., Vol. 275, No. 4, pp. 241–244.

Ahmed, S., Li, Q., Liu, L., & Tsui, A.O. (2012). Maternal deaths averted by contraceptive use: an analysis of 172 countries. *The Lancet* Vol. 380, No. 9837, pp. 111–125.

Aisien, A. O. (2007). Contraception with Levonorgestrel subdermal implants (Norplant) in Benin-city, Nigeria: A 12-year review. *Afr J Reprod Health*, Vol 11, No. 1, pp. 90–97.

Aisien A. O. (2007) Intrauterine contraceptive device (IUCD): Acceptability and effectiveness in a tertiary institution. *Afr J Med Med Sci*., Vol. 36, No. 3, pp. 193–200

Akinwuntan A. L., & Shittu O. B. (2008). Voluntary vasectomy in a Nigerian: A rarity. *Afr J Med Med Sci*., Vol 37, pp. 289–290.

Andrej K., Janez B., & Andrej K. (2011). Introduction to the Artificial Neural Networks, Artificial Neural Networks Kenji Suzuki, Intech Open, DOI: 10.5772/15751. Retrieved on 1 Jan 2018 from: https://www.intechopen.com/books/artificial-neural-networks-methodological-advances-and-biomedical-applications/introduction-to-the-artificial-neural-networks.

Babalola S., Folda L., & Babayaro H. (2008). The effect of a communication program on contraceptive ideation and use among young women in Northern Nigeria. *Stud Fam Plann*. 2008; Vol. 39, No. 3, pp. 211–220.

Bradshaw, C. J. A., & Brook, B. W. (2014). Human population reduction is not a quick fix for environmental problems. PNAS, Vol. 111, No. 46, pp. 16610–16615.

Cavazos-Rehg, P. A., Krauss, M. J., Spitznagel, E. L., Bommarito, K., Madden, T., Olsen, M. A., Subramaniam, H., Peipert, J. F., & Bierut, J. L. (2015). Maternal age and risk of labor and delivery complications. *Maternal and Child Health Journal*, Vol. 19, No. 6, pp. 1202–1211.

DeRose, L., Dodoo, F., Ezeh, A., & Owuor, T. (2004). Does Discussion of Family Planning Improve Knowledge of Partner's Attitude toward Contraceptives? *International Family Planning Perspectives*, Vol. 30, No. 2, pp. 87-93. Retrieved on 1 Jan 2018 from http://www.jstor.org/stable/3181031

Ekabua, J. E., Ekabua, K. J., Ekanem, E. I., & Iklaki, C. U. (2009). Is the process of diagnosing and treating incidental medical findings a barrier to

contraceptive acceptance and use? *J Obstet Gynaecol*, Vol. 29, No. 3, pp. 237–239.

Diaz S. (2002). Contraceptive implants and lactation. *Contraception*, Vol. 65, No. 1, pp. 39-46.

Facts for Family Planning (USAID, 2013). Retrieved on 1 Jan 2018 from https://www.fphandbook.org/factsforfamilyplanning/

Family planning: a global handbook for providers (WHO, CCP, USAID, 2011). Retrieved on 1 Jan 2018 from https://www.fphandbook.org/

Fayyad U.M (1996). Data Mining and Knowledge Discovery: Making Sense Out of Data, *IEEE Expert* Vol. 11, No. 5, pp. 20-25.

Felici, G., & Vercellis, C. (2007). *Mathematical Methods for Knowledge Discovery and Data Mining*. Idea Group Reference.

Frauke G., and Stefan F. (2010). Neuralnet: Training of Neural Networks. *R Journal*, Vol. 2/1 pp 30-38.

Garson G. D. (1991). Interpreting Neural-Network Connection Weights. *AI Expert*. Vol. 6, pp. 46-51.

Haggi D. N. (2003). The Norplant experience in Zaria: A ten-year review. *Afr J Reprod Health*. Vol 7, No. 2, pp. 20–24.

Hastie, T. J., Tibshirani, R., and Friedman, J. (2001). *The Elements of Statistical Learning*. Springer.

Hatcher, R. A., Rinehart, W., Blackburn, R., Geller, J. S., James D. et al. (1997). *The Essentials of contraceptive technology: a handbook for clinic staff* / Robert A. Hatcher [et al.]. Baltimore, MD: Population Information Program, Johns Hopkins University, School of Public Health. Retrieved on 1 Jan 2018 from http://www.who.int/iris/handle/10665/42331.

Kavanaugh, M. L., & Anderson, R.M. (2013). *Contraception and Beyond: The Health Benefits of Services Provided at Family Planning Centers*. New York: Guttmacher Institute.

Ladipo O. A., & Akinso S. A. (2005). Contraceptive implants. *African Journal of Reproductive Health*, 9(1):16–23.

Medical Eligibility Criteria for Contraceptive Use **(**WHO, 2015**).** Retrieved on 1 Jan 2018 from.http://apps.who.int/iris/bitstream/10665/181468/1/9789241549158_eng.pdf?ua=1

National Population Commission (NPC) [Nigeria] and ICF International. (2014). *Nigeria Demographic and Health Survey 2013*. Abuja, Nigeria, and Rockville, MD: NPC and ICF International.

National Population Commission (NPC) [Nigeria] and ICF Macro. (2008). *Nigeria Demographic and Health Survey*. Abuja, Nigeria: National Population Commission and ICF Macro.

Oriji, V. K., Jeremiah I., Kasso T. (2009). Induced abortion amongst undergraduate students of University of Port Harcourt. *Niger J Med*. Vol 18, No. 2, pp. 199-202.

Otoide, V. O., Ononsaye, F., & Okonofua, F. E. (2001). Why Nigeria adolescents seek abortion rather than contraception. Evidence from focus group discussions. *Int Family Plan Perspect* Vol. 27, No. 2, pp. 77-81.

Piatetsky-Shapiro, G., & Frawley, W. J. (1991). *Knowledge Discovery in Databases*. AAAI/MIT.

Vapnik, V. (1998). *Statistical Learning Theory*. Wiley-Interscience, New York.

Yahya, W. B., Oladiipo, M. O., & Jolaye, E. T. (2012). *A Fast Algorithm to Construct Neural Network Classification Models with High-Dimensional Genomic Data. Anal Serial Information*. Vol. X, fasc.39-56.

Witten, I. H., & Frank, E. (2005). *Data Mining: Practical Machine Learning Tools and Techniques with JAVA Implementations* (2nd Ed.), San Francisco: Morgan Kaufmann.