PAPER • OPEN ACCESS

Subscribers' Traffic Internet Bandwidth Usage Capture and Classification Using Android Platform

Subscribers' Traffic Internet Bandwidth Usage Capture and Classification Using Android Platform

A A Adewale, A Ben-Obaje, E E Ekong, A Orimogunje, H K Anabi, O Omoruyi

Electrical and Information Engineering Department, Covenant University, Ogun State, Nigeria

E-mail: ade.adewale@covenantuniversity.edu.ng

Abstract. With the rise in smart devices communicating on internet, there is a huge demand in the delivery of internet bandwidth to fulfil subscribers' aspirations. It is therefore important for internet network providers to understand the subscribers' behavioural pattern in terms of internet bandwidth usage so as to meet up with the continuous rise in its demand. This research introduces the schematics of an android application effectively communicating with a remote database; Firebase cloud service. The classification of the subscribers' internet traffic bandwidth consumption enables the android application to generate dataset of bandwidth utilization patterns of volunteered subscribers' device which are grouped into 4 classes; A, B, C and D representing very high, high, medium and low data usage respectively. The collection of internet bandwidth usage of subscribers was recorded at intervals of every hour into the remote database in Firebase cloud.

Keywords: Android Mobile App, bandwidth usage, subscribers' classification

1. Introduction

Android is a mobile operating system software developed by Google. Google has over 2 billion active devices currently running with the operating system (OS). Taking the largest share in mobile OS industry. Android Applications are managed by the Google play store where they are maintained and updated. Google announced it had more than 3.3 billion applications on the google play store [1]. Internet bandwidth usage of subscribers has been on a huge rise since the invention of the first smartphone. Now internet bandwidth has even grown high since the introduction of Internet of Things (IoT) devices, smart cars, smart homes, and so on [2, 3, 4]. We now live in the information age where a huge percent of the world's population is connected to the internet [5]. Mobile data traffic is continuously on the increase as result of rapid development of wireless access technology and use of smart devices which is expected to lead to an explosive growth of data in heterogeneous cellular networks [6, 7, 8]. It is significant for network operators to expand the capacity of their networks to avoid congestion and overload to guarantee users' satisfaction [3, 4, 10, 16].

2. Literature review

Android is a Linux based operating system that relies on Linux kernel for its security, memory management, network stack and driver model [5]. Android is an open source framework where any develop can develop and contribute application to its community [9, 10]. Android data storage can be secured only if the user does not root the device [13]. Root the device grant write access to system files and storage [6, 11, 12]. Firebase is a cloud drive service provider that provides robust backend functions to developers that build applications for the android OS [7, 13, 14]. Firebase database stores data in JavaScript Object Notation (JSON) syntax comprising of objects and string in arrays. Firebase real time database has an application program interface (API) service which is supplied to application developers upon activation of a Firebase cloud account [8, 15].

3. Methodology

The system comprises of a mobile application component, a learning component which is supported by an artificial neural network. The system was developed to provide an effective cellular data usage in a bid to improve data/bandwidth accessibility to all users ranging from regular users to power users. The android application used for data collection was designed with android architecture components which is a collection of libraries that help in the design of robust, testable, and maintainable apps. The data capture from each user was securely stored in a database and converted to a huge dataset which can be classified and analyzed.

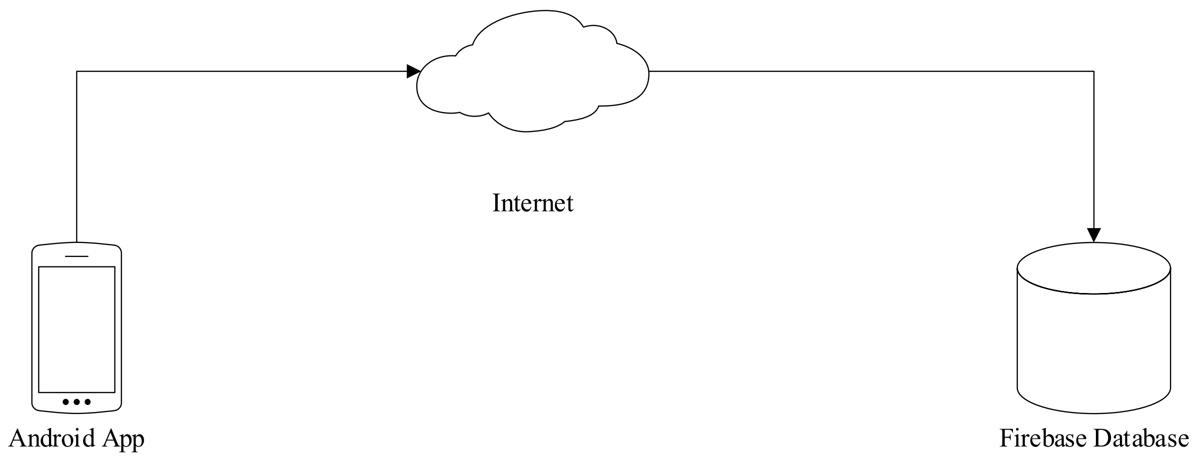

Figure 1. Components Block Diagram

Figure 1 shows the block diagram of the components of the android application where each subscriber effective communicates with the remote database Firebase which is in the cloud.

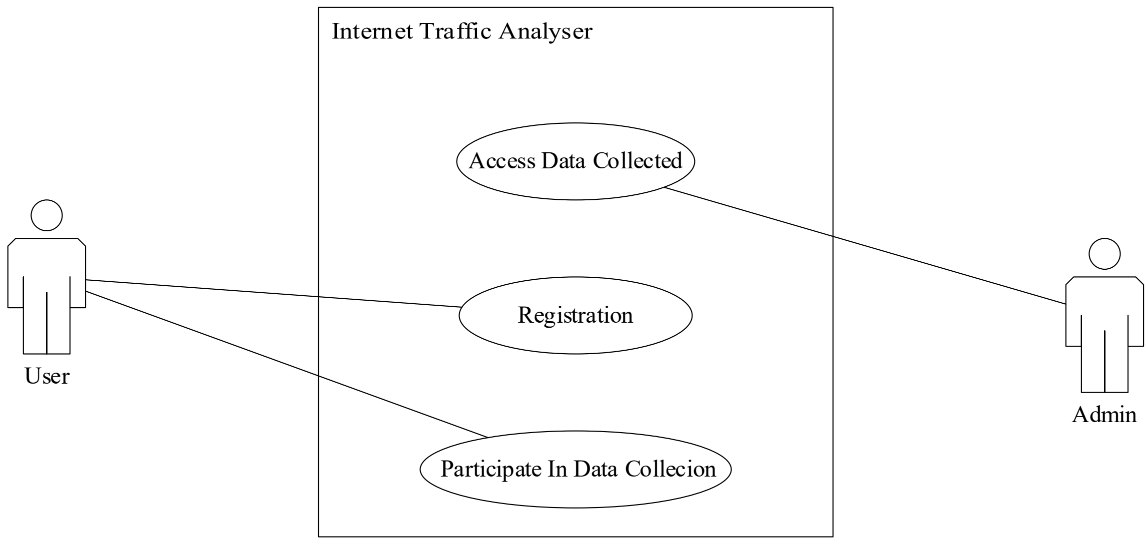

Figure 2. Use Case Diagram of the internet traffic analyzer

3.1 Actors
In the diagram figure 2 above two actors are present and can interact with the android system. The first actor represents that user and second actor is the admin. The user is a volunteered participant who downloads and install the mobile app on his phone and the app captures his data traffic seamlessly and without any inconvenience. The admin has the privilege to access the data traffic captured and stored in the database.

3.2 Use Cases
Three actions were identified as necessary in the solution.
3.2.1 Access Data Collected
This part of the system gives admin access to the Firestore database via the Google Firebase web console. Data can be queried in parts or in completions and download to either json or xml format.
3.2.2 Registration
This action enables users to register on the database with their respective Gmail accounts through the Google identity Server hence generating a UUID (Universally Unique Identifier) for all the participating user. The data collected must relate all the traffic information collected to the different respective users.
3.2.3 Participate Data Collection
This part notifies the user with a special permission dialog acknowledging that traffic and privacy information will be collected for this research purpose.

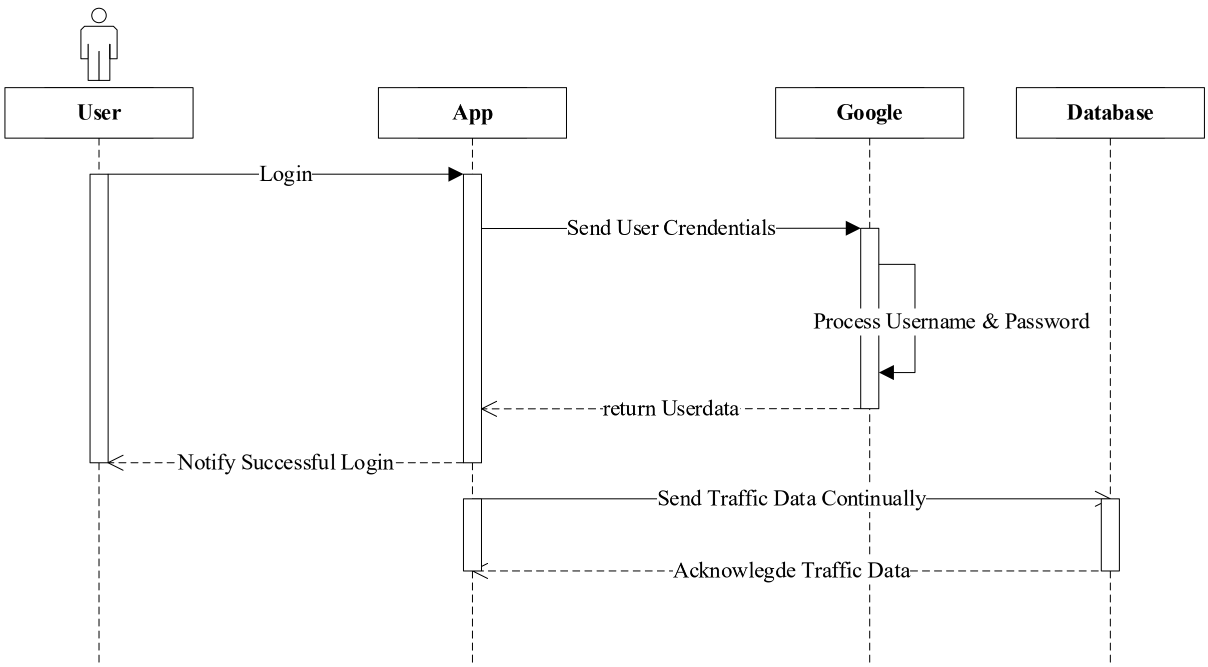

Figure 3. Sequence Diagram

Figure 3 is a sequence diagram showing the user scenario with the android application for data capture. For the first action the user attempts to login into the android application where the user selects his google account to be registered and the credentials will be authenticated on the Google Identification Server. The Google Server then replies the Application with a universally unique identifier (UUID) object to register the user with on the database to be used for data collection. For security risk of data and privacy exposure emails and passwords will not be collected but rather an encrypted UUID. Once the user completes his registration the user will be notified to exit (not Force Stop) the program and go about carrying regular device operation. With a background service injected into the application the application sends traffic consumed within an interval through the internet and saves it in the Firestore database.

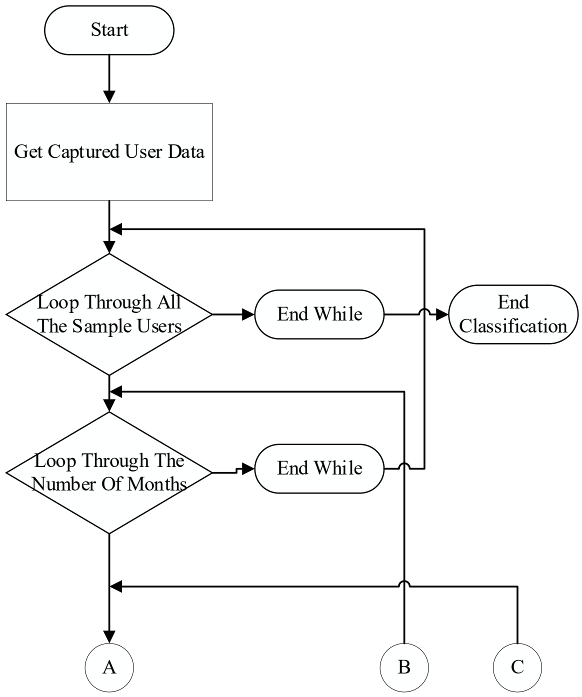

Figure 4. Top left section of the mobile app flowchart

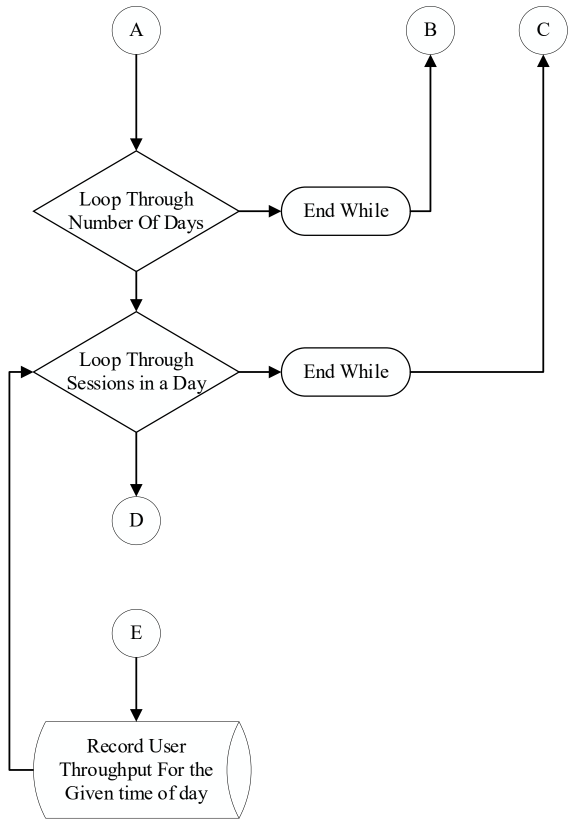

Figure 5. Bottom Left Section of the Mobile Flowchart for daily sessions

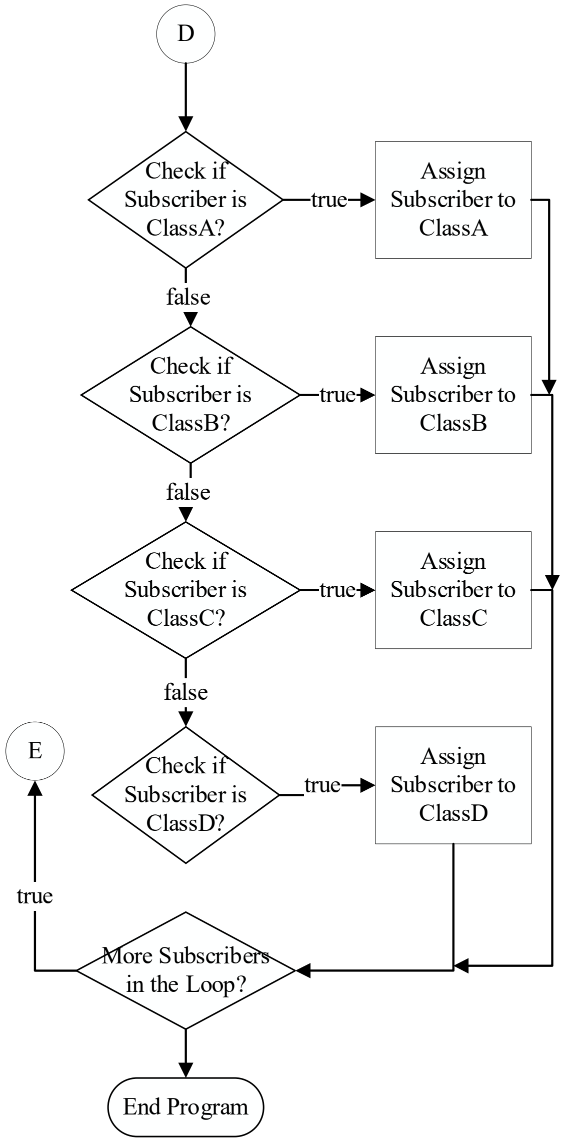

Figure 6. Right Section of the Mobile App Flowchart showing classification

The above flowchart in figure 4-6 shows the process, decisions and loops carried out in the background of the android application while the subscriber uses his smart device without interruption.

Step1: The captured data from the log file is injected.
Step2: Loop through all the available sample users.
Step3: Loop through the number of sampled months
Step4: Loop through the number of sampled days in each month.
Step5: Loop through the number of sampled sessions in each day
Step6: Checks if the user is in the class A
Step7: Checks if the user is in the Class B
Step8: Checks if the user is in the class C
Step9: Checks if the user is in the class D

Step10: Checks if there are more users in the loop
Step11: Records the results of every user in the database

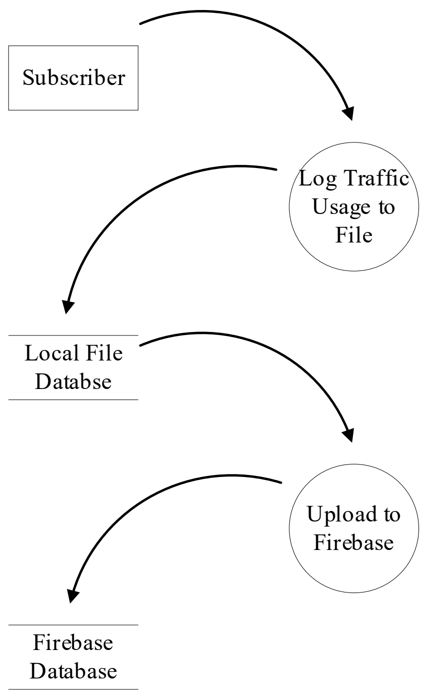

Figure 7. Dataflow Diagram

The diagram above in figure 7 shows the data flow diagram. The diagram details the movement of storage data while the subscriber is interacting with the application.

4. Results and discussion

Figure 8 to figure 11 are screenshots of the app running on a volunteered mobile subscriber device and is interacting with that application. The screenshots show how the user goes through the process of registering on the database and notifies them not to terminate the process.

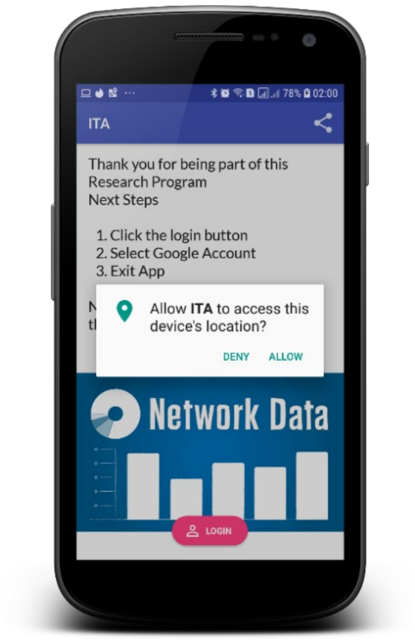

Figure 8. Permission Dialog

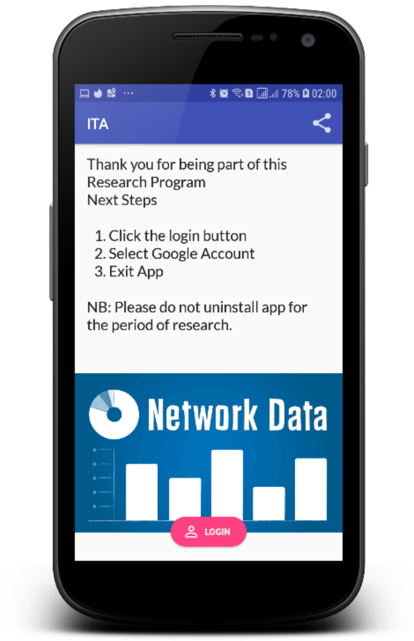

Figure 9. Login Page

This first screenshot figure 8 shows a dialog that requests the user to allow access to special location permissions in other to get accurate reading from the cellular antenna. This next screenshot figure 9 shows the home screen that instructions on how to keep the app running through the time of the research.

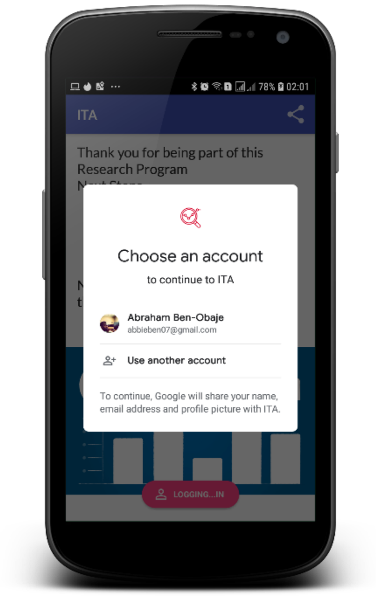

Figure 10. Login Dialog

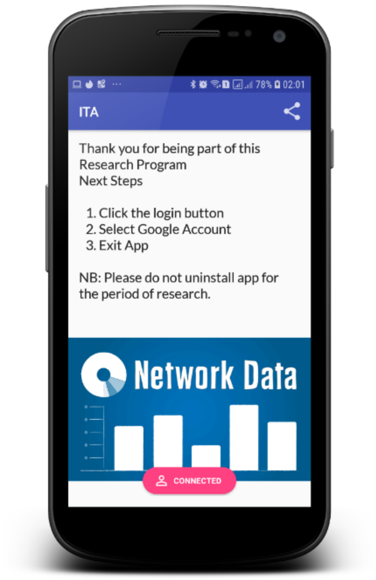

Figure 11. Home Page

The above screenshot in figure 10 shows a dialog of the user's google login to uniquely identify all the users using the google UUID (Universal Unique Identification) and the user's Gmail address.
Figure 11 shows that the current user has successfully registered on the central logging database and can exit the app. While data collection happens in the background unnoticed by users.

Table 1. Sample of Data Captured by the Android App

	Hour 1	**Hour 2**	**Hour 3**	**Hour 4**	**Hour 5**	**Hour 6**

Subscriber 1	15187363	5094151	4962967	16206343	31217766	2349672
Subscriber 2	508187	1710253	11039681	11491407	14919350	1290689
Subscriber 3	11950268	4140947	1859896	5159517	8470140	7996821
Subscriber 4	16580960	19284915	12445716	2443831	10177103	1582108
Subscriber 5	5026314	3449965	4762974	15285140	4582130	5262347
Subscriber 6	10267271	8813847	4391928	3041241	10058617	264923
Subscriber 7	4674058	4881098	2990624	1295985	10576064	4147763
Subscriber 8	2849428	5414198	12086371	9551831	8369403	4653430
Subscriber 9	7502996	7323398	9830629	4475321	12936556	15257698
Subscriber 10	4547083	7580535	3843376	22813627	16857034	2774415

Table 1 shows a small segment of the data captured front the remote database Firebase remote database. Each column represents a unique user, each row represents a time interval and each cell represents the internet traffic data consumed within the Time interval.

Table 2. Sample of Classified Data based level of bandwidth usage

	Hour 1	**Hour 2**	**Hour 3**	**Hour 4**	**Hour 5**	**Hour 6**
Subscriber 1	3	2	2	3	4	1
Subscriber 2	1	1	3	3	3	1
Subscriber 3	3	2	1	2	3	3
Subscriber 4	3	4	3	1	3	1
Subscriber 5	2	2	2	3	2	2
Subscriber 6	3	3	2	2	3	1
Subscriber 7	2	2	2	1	3	2
Subscriber 8	2	2	3	3	3	2
Subscriber 9	2	2	3	2	3	3
Subscriber 10	2	2	2	4	3	2

Legend: 1 = Class A, 2 = Class B, 3 = Class C, 4 = Class D
Each column represents an hour interval of the data captured and classified, each row represents a subscriber from the Table 1.

5. Conclusion

The implementation of this research provides a means to capture internet traffic usage of subscribers and adequately classify them using a smart methodology with the aid of the android platform and the Google Firebase cloud service**.** The classification was done by MATLAB scripting which groups the subscribers to four (4) different groups based on their level of data consumption. The data acquired from this study has several applications among which are for network traffic analyses and decongestion of mobile operators network through Wi-Fi offloading [17].

Acknowledgments
Authors of this article would like to thank the management of Covenant University for financing the publication of this article.

References

[1] Meiliana, Septian I, Alianto R S and Daniel 2018 Comparison Analysis of Android GUI Testing Frameworks by Using an Experimental Study *Proc. of 3rd Int. Conf. on Computer Science and Computational Intelligence* **135** pp. 736–48
[2] Singh S and Singh N 2015 Internet of Things(IoT): Security Challenges,Business Opportunities and Reference Architecture for E-Commerce *Proc. of Int. Conf. on Green Computing and Internet of Things (ICGCIoT)* pp 1577–81.
[3] Adewale A A, Ayodotun S I, Atayero A A, John S N, Okesola O and Ominiabohs R R 2019 Nigeria's Preparedness for Internet of Everything: A Survey Dataset from the Work-force Population *Data in Brief (Elsevier)* **23**
[4] Ibhaze A E, Ajose S O, Atayero A A, Idachaba F E 2016 Developing Smart Cities Through Optimal Wireless Mobile Network *Proc. of Int. Conf. on Emerging Technologies and Innovation Business Practices for the Transformation of Societies (Balaclava) IEEE* pp 38-42
[5] Sun, Yunchuan, Xia Y, Song H, and Bie R 2014 Internet of Things Services for Small Towns *Proc.of Int. Conf. on Identification, Information and Knowledge in the Internet of Things IIKI pp* 92–95.
[6] Ahlgren, Bengt, Hidell M, and Edith C H 2016. Internet of Things for Smart Cities: Interoperability and Open Data *IEEE Internet Computing* **20(6)** pp 52-6
[7] Papetti A, Capitanelli A, Cavalieri L, Ceccacci S, Gullà F, and Germani M 2016 Consumers vs Internet of Things: a systematic evaluation process to drive users in the smart world *Proc. of 26th CIRP Design Conference Elsevier* **50** pp 541-6
[8] John S N, Ibikunle F A and Adewale A A 2008 Performance Improvement of Wireless Network Based on Effective Data Transmission *Proc. of IET Int. Conf. on Wireless, Mobile and Multimedia Networks (Beijing)* IEEE pp 134-37
[9] Adewale A A, Adagunodo E R, John S N and Ndujiuba C U 2016 A Comparative Simulation Study of IP, MPLS, MPLS-TE for Latency and Packet loss Reduction over a WAN *Int. Journal of Networks and communications* **6** pp 1-7
[10] Wang Y, Yi Y N, Zhou H, Dong Y, and Zhiyuan J 2017 The Improvement of the Trustworthiness of Android App Stores in China *Proceedings - Asia-Pacific Software Engineering Conference, APSEC* pp 357–60
[11] Popoola S I, Faruk N, Atayero A A, Oshin M A and Adigun M 2017 5G Radio Access Network Technologies: Research Advances *Proc. of World Congress on Engineering and Computer Science (San Francisco) **1***
[12] Adewale A A, John S N and Adagunodo E R 2016 Performance Comparison of Dynamic Guard Channel with Buffered Prioritized Scheme for Mobile WiMAX Network", in the proceedings of the World Congress on Engineering (WCE) *Proc. of World Congress on Engineering (London)* **1** pp 566-70
[13] Guo, Weiming, Shunxiang W, and Dengyou W 2017 A Forensics Method for Android Devices Based on the Technique of Temporary Root Proc. of *12th Int. Conf. on Computer Science and Education* (Iccse) pp 502–5.

[14] Adewale A A, Adagunodo E R, John S N, Matthews V O and Adelakun A A 2016 Performance Evaluation of Dynamic Guard Channels Assignment with Queue and Prioritized Schemes *Proc. of Mobile Computing Conf. (Las Vegas)* IEEE pp 1059-63

[15] Adewale A A, Ike D U, Ndujiuba C N and John S N 2014 Improvement of quality of service over a wide area network using multiprotocol label switching traffic engineering *Int. J. of Computer Application* **88** 14-8

[16] Adewale A A, Adagunodo E R and John S N 2016 Improving Prioritized Handover Performance for Mobile WiMAX by Dynamic Guard Channel Allocation and RSS Quality Factor *Proc. of IEEE SAI Computing Conf. (IEEE)* pp 669-74

[17] Peng Y T, Sou S I, Tsai M H and Lin C S 2017 Multipath mobile data offloading of deadline assurance with policy and charging control in cellular/WiFi networks *Computer Networks, **129*** pp 17-27