American Journal of Engineering Research (AJER)
E-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-7, Issue-12, pp-105-115
www.ajer.org
Research Paper Open Access

Internet of Things: Implementation Challenges in Nigeria

Iwayemi A.
(Department of Computer Engineering, The Federal Polytechnic, Ile-Oluji, Nigeria)
Corresponding Author: Iwayemi A.

ABSTRACT: *The Internet of Things (IoT) can be defined as a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. It is simply the interconnection via the internet of computing devices embedded in everyday objects enabling them to send data and receive data. The aim of this research is to review the implementation challenges of the implementation of Internet of Things (IoT) in Nigeria. The methodology employed to carry out this research includes Collating information from Journal papers and other relevant materials on IoT, Browsing the Internet through search engines like Google, Administering questionnaire titled "Internet of Things (IoT) in Nigeria Implementation Challenges" to collect information from professionals; Evaluating the completed questionnaires using Statistical Packages for Social Sciences (SPSS) and presentation of results in tables and chart. The findings from the analysis of data turned out that, each of the following, among others, is a factor challenging the implementation of IoT in Nigeria: Fraud, Power supply, Religion, Technical Know-how of how to implement IoT, Cost of Implementing IoT, Tools, equipment and other raw materials necessary for carrying out IoT, Nigeria Government, Cyber Attack, Privacy, Security and Fear of Jobloss/Joblessness. As the IoT is expected to drastically increase productivity, the understanding of the barriers stated in this paper is expected to be an eye-opener to the related solutions.*

KEYWORDS: *Cyber-attack, IoT, Privacy, Security, Tools.*

Date of Submission: 01-12-2018 Date of Acceptance: 31-12-2018

I. INTRODUCTION

[11] said the expression "Internet of Things" was firstly used by an MIT executive director, Kevin Ashton, back in 1999. At the time, the sensors were becoming cheaper and more digitalized, which made Ashton to start thinking about the next logical step for the ICT era: connecting the things via Internet [4]. The very basic idea was to utilize on the existing Radio-Frequency Identification (RFID) technology by equipping all the objects in with identifiers and wireless connectivity, enabling them to communicate with each other via Internet. From that point onwards, the term IoT has been expanding and definitions was modified in various ways. Internet of Everything (IOE) is a term that Cisco uses to explain an interconnected network of not just objects, but also people, places and things [6] Then there is Industrial Internet of Thing (IIoT) which, as the name suggests, refers to the IoT in the industrial sense, where the primary focus is on connecting the machines involved in the manufacturing process [12]. Bearing in mind that the term IIoT is considered as part or a subcategory of IoT, in order to avoid any confusion, this paper will use the basic term, IoT, as it encompasses all the other terms.

The Internet of Things (**IoT**) can be defined as a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. According to [8], this is the concept of basically connecting any device with an ON and OFF switch to the Internet (and/or to each other). Any object simply means everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. The IoT is a giant network of connected "things" (which also includes people). The relationship includes between people-people,

people-things, and things-things. The new rule for the future is going to be, "Anything that can be connected, will be connected."

The global challenges of IoT are really not the same as the peculiar challenges faced in the implementation of it in Nigeria. Nigeria, being a special country because of the number of tribes, education level of people, political scenario, import/export ratios, level of manufacturing industries, unemployment level and so on has its special challenges to implementing IoT. Hence, IoT is already embraced by many countries but having no patronage or low patronage in Nigeria.

This research looks into the various implementation challenges in the world and also administer a questionnaire in an academic institution where Cisco trainings and IoT are offered as a Courses in Nigeria to analyse the various challenges. Fig.1. and Fig. 2.show IoT and IoT Communication Infrastructure respectively.

Fig.1. Internet of Things (source:https://www.rfpage.com/challenges-in-internet-of things-implement

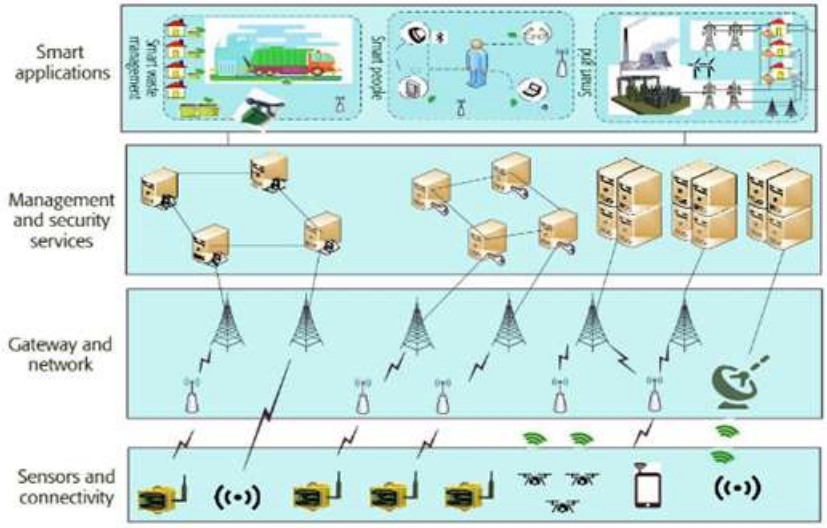

Fig. 2. IoT Communication Infrastructure [5, 12]

The second section of this paper describes the Analysis and Critical Literature. The third describes theresults and discussion, and finally the conclusion is discussed in the fourth section.

II. ANALYSIS AND CRITICAL LITERATURE

Steps of Research

Several steps were taken to achieve the aim of this research. These steps are necessary in drawing a germane conclusion on the subject matter. The steps employed to carry out this research are enumerated below:

Step One: Collating information from Journal papers and other relevant materials on IoT

Pieces of information were collected from materials including reputable journals, conference proceedings, books, magazines and every relevant material that provides information on IoT. Materials from organizations like International Institute of Electrical and Electronic Engineering (IEEE), Association for

Computing Machineries (ACM), British Computer Society, Nigeria Computer Society (NCS), Computer Professionals of Nigeria, International Journal of Computer Science and Telecommunications (IJSCT), Cisco Networking Academy and other relevant ones were thoroughly studied to understand the concept. Newspapers also were consulted.

Step Two: Surfing the Internet through search engines like Google and Google scholar

Several online publications were consulted to get the present-day views of the topic sentence. Some of the sources visited are cited and listed in the List of References. Google is a general all-purpose search engine whereas Google Scholar focuses on scholarly literature. Google scholar materials include articles, theses, books, abstracts, U.S. court opinions, and patents, found on the websites of academic publishers, professional societies, online repositories, universities and more. By scholarly literature, Google means publications that are based on the results of research or studies. Google, on the other hand, has a broader scope, and retrieves resources regardless of where online they come from. Resources in a Google search do not have to be scholarly, and do not have to be based on research.

Step Three: Reviewof Related Literatures in tabular form

Much information was collected already among which there existed highly useful notions of relevant discussion. A Presentation of collated literatures in a Meta data results in tables and figures was reported. All the literatures were carefully studied while some critical ones are keenly reviewed and summarized in Table I.

Table I: Review of Related Critical Literatures in Tabular Form

S/N	AUTHOR	TITLE	SOURCE	STRENGTH
1	Restuccia and Melodia, 2018	Securing the Internet of Things:New Perspectives and Research Challenges	IEEE Internet Of Things Journal	IOT Authentication, wireless networking and IOT data aggregation
2	Beecher, 2018	Three IoT implementation challenges and how to overcome them	Internet	Identified Security risk, senior executive buy-in and choosing the right technology
3	Banafa, 2017	Three Major Challenges Facing IoT	Internet	Identified major challenges: technology, business and society
4	Tomic, 2017	Benefits of Implementing IoT in Manufacturing Production	Unpublished M.Sc. Thesis	Predictive maintenance Data analysis, higher customer satisfaction, securing a comp adv.
5	Tomic, 2017	Barriers to implementing IoT in manufacturing production	Internet	ROI, Cyber-security, cultural resistance, structural problems

Table I: Review of Related Critical Literatures in Tabular Form (Contd.)

S/N	AUTHOR	TITLE	SOURCE	STRENGTH
6	Yaqoob, et al. 2017	IoT Communication Infrastructure	IEEE Wireless. Communication	IoT Communication Infrastructure
7	Burhanuddin, et. al. 2017	Internet of Things Architecture: Current Challenges and Future Direction of Research	International Journal of Applied Engineering Research	Scalability, interoperability and security.
8	Ndubuaku, M. and Okereafor, D. (2015).	Internet of Things for Africa: Challenges and Opportunities	International Conference on Cyberspace Governance - CYBERABUJA2015	Identified power supply, High poverty rate, network capacity constrain, illiteracy, lack of local content, low internet penetration rate, interoperability and standard, data management, security issues and privacy issues

Step Four: Administering questionnaire titled: "Internet of Things (IoT) in Nigeria: Implementation Challenges" to collect information from Nigerian professionals.

Questionnaires were administered to professionals with high qualifications from Higher Institutions. The respondents are people who lecture at the Higher Institution. An Institution where IoT is being taught was chosen and the lecturers were served. Questions ranging from the qualifications of the respondents to the divers kinds of implementation challenges of IoT in Nigeria were designed. This questions are to enable us know the various level of hindrances that each of the factors creates in militating against the implementation.

Step Five: Evaluating the completed questionnaires using Statistical Packages for Social Sciences (SPSS).
The questionnaires were coded and analyzed to make some findings. Frequency tables were generated from the series of responses from the Instructors.

Step Six: Making Findings and Concluding
Discussed the results of the research, reported the findings, drew conclusion and made recommendations from evaluated materials.

III. RESULTS AND DISCUSSION

A.Specific Findings

From the review of literature and other researches, the following findings were deduced:

1. Apart from the global challenges that make implementation of Internet of Things (IoT), Nigeria has it own special challenges among which are power supply, Religion, Government, Tools and Cost.
2. It turns out thatthe challenges of implementing IoT like security are less challenge than the technology infrastructure such as power supply, good governance, availability of tools, cost and knowledge in Nigeria. Power supply and governance have higher precedence in terms of implementing anything in Nigeria than any other thing. [1], [2], [10],[7],[3].[10] affirmed that Technology infrastructure is a vital prerequisite for economic, industrial and technological development and growth. The paper revealed that Nigeria with population of over 140 million was only able to generate less than 3000 MW as against over 10,000 MW needed to transform the economy of the country. The paper argued that this precarious situation has serious negative implications for the operations of industrial sector in the country. This situation represents a major setback on the country's quest for industrial development.
3. Security in the global sense is not the same as the security in the context of Nigeria problem.Security in the global sense talks about electronic, data and digital security whereas physical security is a greater ill in Nigeria.Common security treats in Nigeria include serial bombing, hostage taking, armed robbery, cold-blooded killings and ethno-religious conflicts traceable to militant groups with conflicting ideological, political and religious agenda.
4. Lack of tools is the greatest challenge militating against IoT in Nigeria. Raw materials are tools needed to design the embedded systems, sensors and the internet. For instance, many sensors were available and getting cheap, hence the reasons for the thought of IoT but in Nigeria, sensors are very difficult to get in the market and obviously in the country. It is difficult to practice or get into full design since the components needs are not easily accessible; it takes longer time when they are ordered from outside country.
5. Solar energy is set to become the biggest trend. Installing slim and transparent solar panels on phones, cars and even buildings has already started providing consumers to keep going without ever having to worry about looking for the nearest plug. Other technologies are being explored: Electromagnetic Energy to recharge devices, Thermal and RF are also being introduced to power devices and stretch batteries' lives. Wi-Fi based sensors have been developed to run on 2xAA batteries for over a year. Glass material that has the properties to double a smartphone battery life [9].

B.General Findings

The findings from the analysis of data turn out that, each of the following, among others, is a factor challenging the implementation of IoT in Nigeria and the results of twenty questionnaires distributed is represented in tables and bar charts :

1. Fraud

Table II: Frequency table showing the description of Fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5	1	5.0	100.0	100.0
Missing	System	19	95.0		
Total		20	100.0		

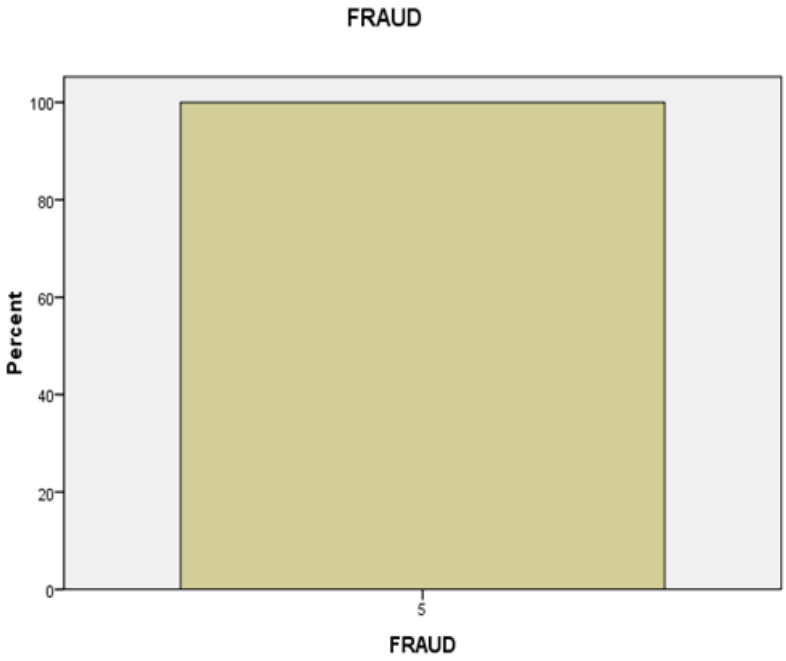

Fig.3. Bar Chart showing the description of Fraud

2. Power Supply

Table III: Frequency table showing the description of Power Supply

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	5.0	50.0	50.0
	5	1	5.0	50.0	100.0
	Total	2	10.0	100.0	
Missing	System	18	90.0		
Total		20	100.0		

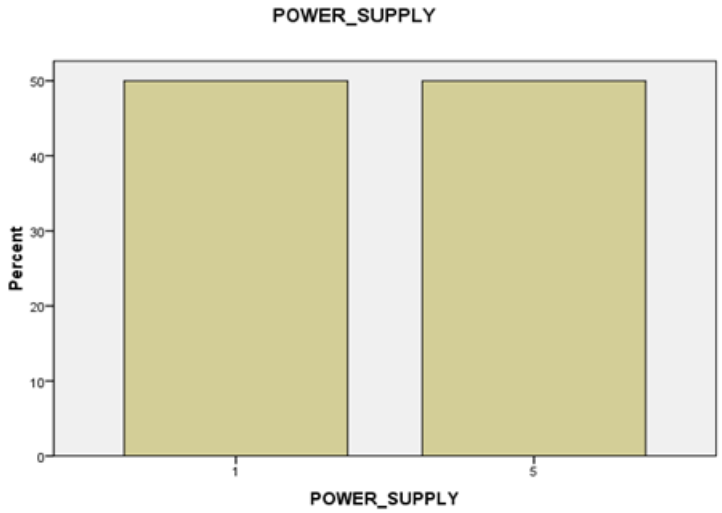

Fig. 4. Bar Chart showing the description of Power Supply

3. Religion

Table IV: Frequency table showing the description of Religion

	Position	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	6	1	5.0	5.3	5.3
	7	1	5.0	5.3	10.5
	8	2	10.0	10.5	21.1
	3	3	15.0	15.8	36.8
	2	4	20.0	21.1	57.9
	10	8	40.0	42.1	100.0
		19	95.0	100.0	
Missing	System	1	5.0		
Total		20	100.0		

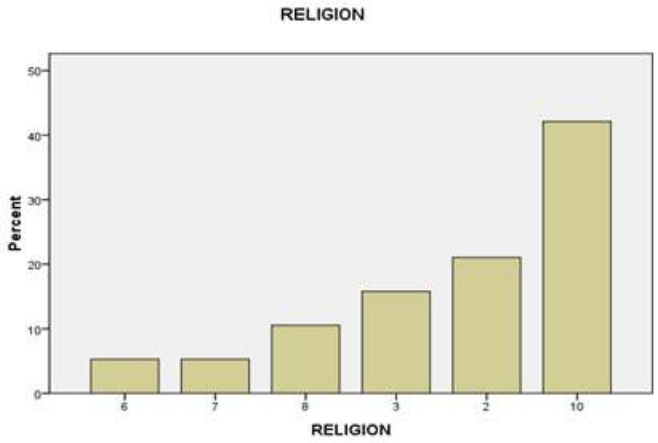

Fig. 5. Bar Chart showing the description of Religion

4. Cost

Table V: Frequency table showing the description of Cost

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	6	1	5.0	5.0	5.0
	7	1	5.0	5.0	10.0
	3	3	15.0	15.0	25.0
	2	4	20.0	20.0	45.0
	5	4	20.0	20.0	65.0
	1	7	35.0	35.0	100.0
	Total	20	100.0	100.0	

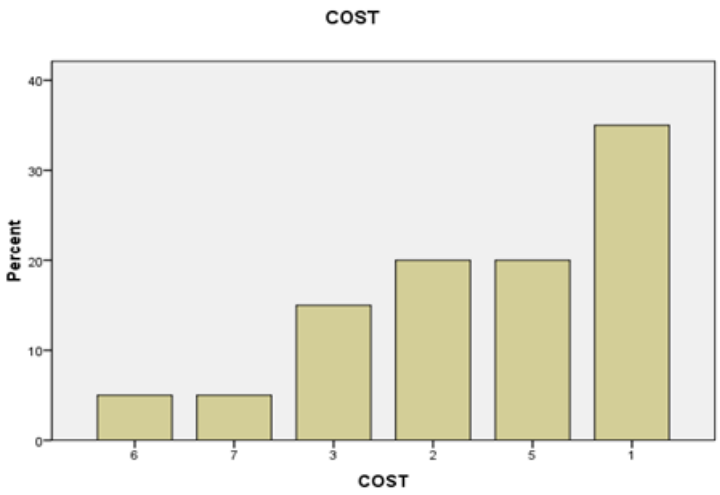

Fig.6. Bar Chart showing the description of Cost

5. Knowledge

Table VI: Frequency table showing the description of knowledge

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5	1	5.0	5.0	5.0
	6	2	10.0	10.0	15.0
	3	3	15.0	15.0	30.0
	4	4	20.0	20.0	50.0
	1	5	25.0	25.0	75.0
	2	5	25.0	25.0	100.0
	Total	20	100.0	100.0	

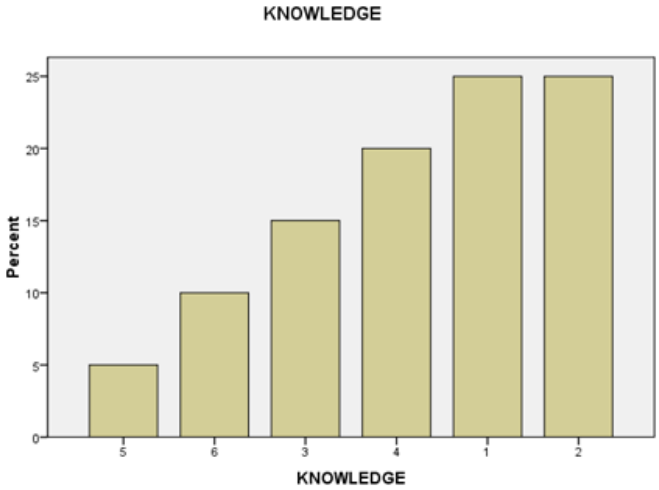

Fig.7. Bar Chart showing the description of Knowledge

6. Tools

Table VII: Frequency table showing the description of Tools

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	1	5.0	5.0	5.0
	5	1	5.0	5.0	10.0
	2	5	25.0	25.0	35.0
	3	5	25.0	25.0	60.0
	1	8	40.0	40.0	100.0
	Total	20	100.0	100.0	

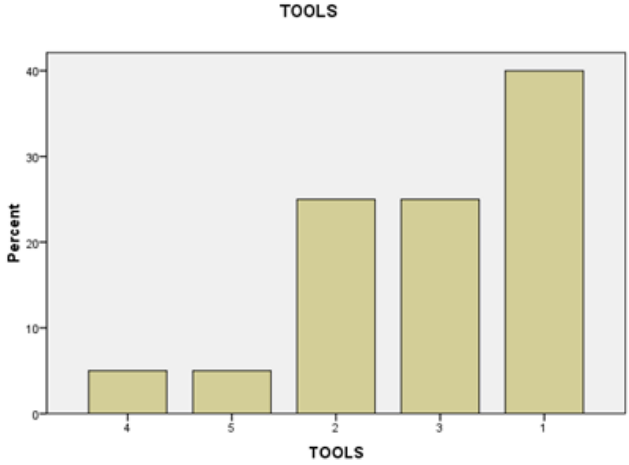

Fig.8. Bar Chart showing the description of Tools

7. Government

Table VIII: Frequency table showing the description of Government

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	5.0	5.0	5.0
	5	1	5.0	5.0	10.0
	7	1	5.0	5.0	15.0
	8	1	5.0	5.0	20.0
	10	2	10.0	10.0	30.0
	3	3	15.0	15.0	45.0
	4	4	20.0	20.0	65.0
	2	7	35.0	35.0	100.0
	Total	20	100.0	100.0	

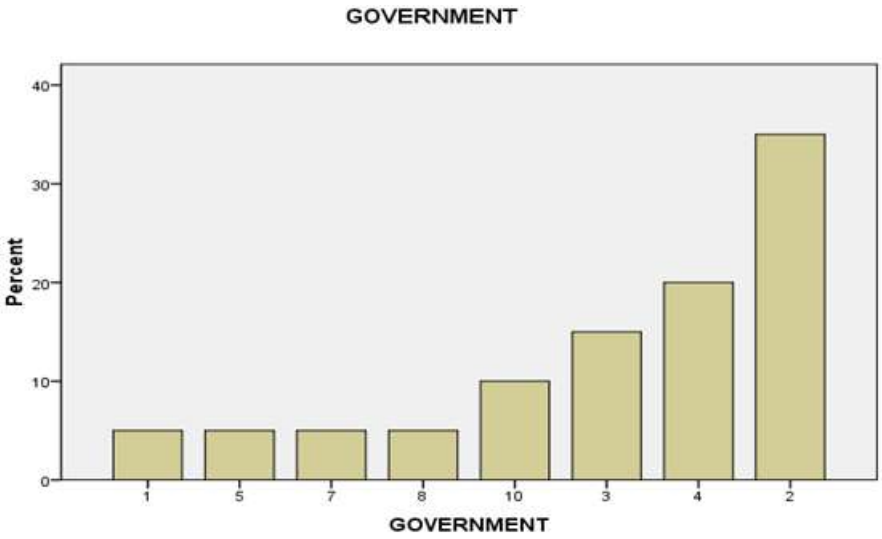

Fig.9. Bar Chart showing the description of Government

8. Cyber Attack

Table IX: Frequency table showing the description of Cyber Attack

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	10	1	5.0	5.3	5.3
	3	2	10.0	10.5	15.8
	6	2	10.0	10.5	26.3
	4	3	15.0	15.8	42.1
	2	4	20.0	21.1	63.2
	1	7	35.0	36.8	100.0
	Total	19	95.0	100.0	
Missing	System	1	5.0		
Total		20	100.0		

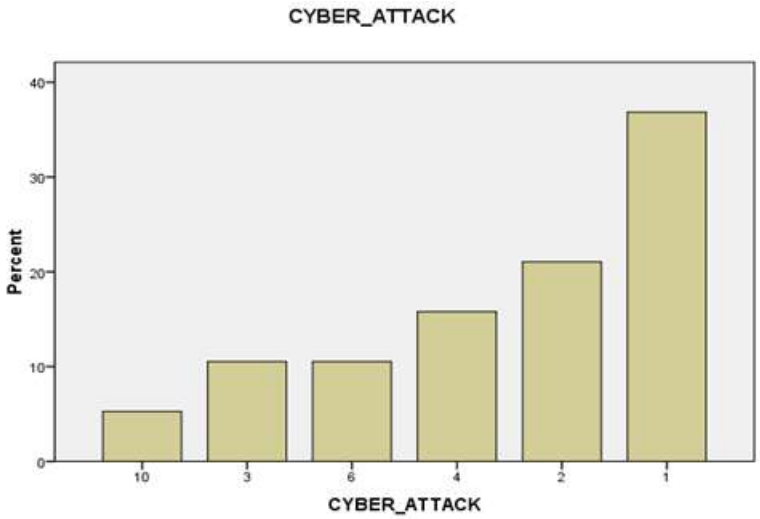

Fig. 10. Bar Chart showing the description of Cyber Attack

9. Security

Table X: Frequency table showing the description of Security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	1	5.0	5.0	5.0
	7	2	10.0	10.0	15.0
	8	3	15.0	15.0	30.0
	1	4	20.0	20.0	50.0
	2	5	25.0	25.0	75.0
	3	5	25.0	25.0	100.0
	Total	20	100.0	100.0	

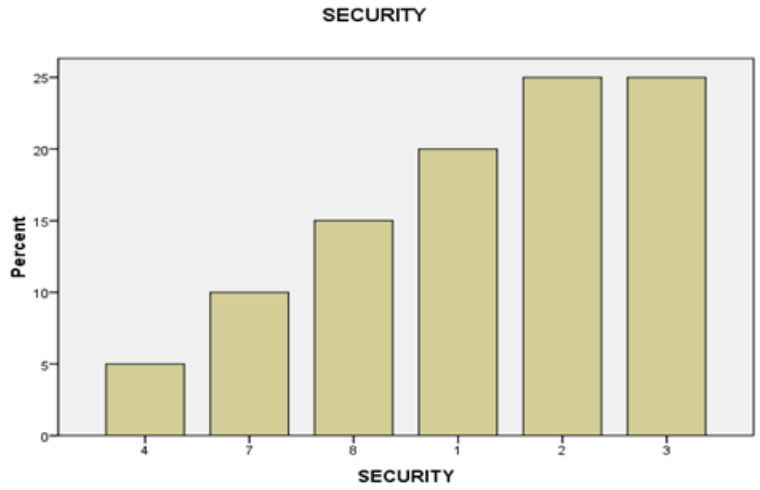

Fig. 11. Bar Chart showing the description of Security

10. Privacy

Table XI: Frequency table showing the description of Privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	5.0	5.3	5.3
	8	1	5.0	5.3	10.5
	9	1	5.0	5.3	15.8
	7	2	10.0	10.5	26.3

	2	3	15.0	15.8	42.1
	4	3	15.0	15.8	57.9
	5	3	15.0	15.8	73.7
	3	5	25.0	26.3	100.0
	Total	19	95.0	100.0	
Missing	System	1	5.0		
Total		20	100.0		

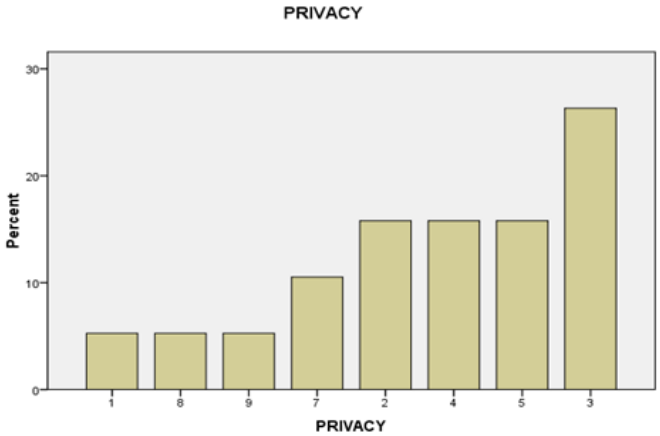

Fig. 12. Bar Chart showing the description of Privacy

11. Job loss and Joblessness

Table XII: Frequency table showing the description of Joblessness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	9	1	5.0	5.0	5.0
	10	1	5.0	5.0	10.0
	4	2	10.0	10.0	20.0
	5	2	10.0	10.0	30.0
	1	3	15.0	15.0	45.0
	3	3	15.0	15.0	60.0
	7	3	15.0	15.0	75.0
	2	5	25.0	25.0	100.0
	Total	20	100.0	100.0	

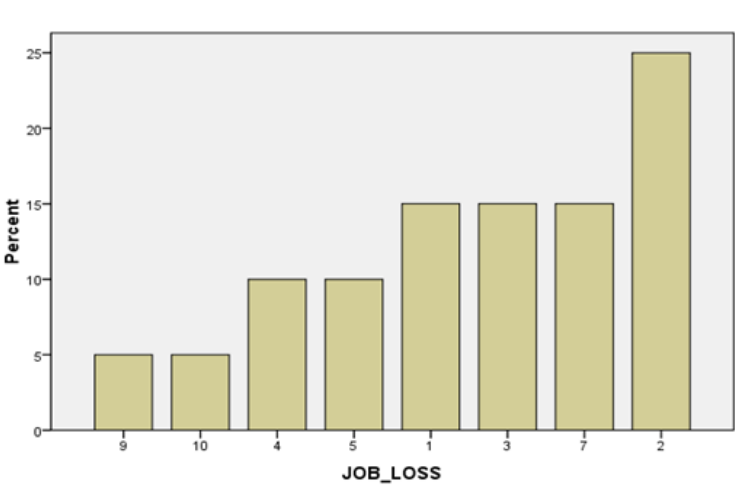

Fig. 13. Bar Chart showing the description of Joblessness

IV. CONCLUSION

There are critical implementation challenges of IoT in Nigeria in addition to the global challenges of security, privacy, technology business etc. These critical challenges are peculiar to Nigeria as a nation such that if the global fears of IoT are removed, implementing IoT in Nigeria is still a day-dream and is highly achievable in Nigeria. Nigeria has the potential of being the highest country in the implementation of IoT if the challenges are removed. Today, Nigeria is one of the highest users of mobile devices so the problem is not that the people are not accepting IoT but rather that the people are not enabled to create or be part of IoT.

REFERENCES

[1]. Achebe, C.: TheTrouble with Nigeria. Heinemann Educational Publishers. Portsmouth, USA, (1998).
[2]. Adenikinju, A.: Electric infrastructure failures in Nigeria: a survey-based analysis of the costs and adjustment responses. Journal of Energy Policy, vol. 32(14), pp. 1519-1530 (2003).
[3]. Aduwa-Ogiegbaen, S., Iyanu, E.: Using Information and Communication Technology in Secondary Schools in Nigeria: Problems andProspects. Journal of Educational Technology & Society, vol. 8(1), pp.104-112 (2005).
[4]. Ashton, K.: That Internet of Things. RFiD Journal,vol. 22(7), pp. 97-144 (2009).
[5]. Burhanuddin, M., Mohammed, A., Ismail, R., Basiron, H.: Internet of Things Architecture: Current Challengesand Future Direction ofResearch. International Journal of Applied EngineeringResearch, vol. 12(21), pp.11055-11061 (2017).
[6]. Cisco: The IoT threat environment. Available online at: http://theinternetofthings.report/Resources/Whitepapers/4c7c4eca- 616-45c3-aac8- bff6031cadc9_IoT%20Threat%20Environment.pdf, Accessed on 1st May 2018, (2015).
[7]. Iwayemi, A.: Nigeria's Dual Energy Problems: Policy Issues and Challenges. International Association for Problem Energy Economics. Cleveland. USA(2008).
[8]. Morgan, J.: A Simple Explanation of the Internet of Things. Available online at: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#6ffdffe01 d09, Accessed on 1st May 2018, (2014).
[9]. Ndubuaku, M., Okereafor, D.: Internet of Things for Africa: Challenge and Opportunities. *In:* proceedings of 2015 International Conference on Cyberspace Governance-CYBERABUJA2015. PP.23-31 (2015).
[10]. Okafor, E.: Development Crisisof Power Supply and Implications forIndustrial Sector in Nigeria. Journals of Studies of Tribes and Tribals, vol. 6(2) (2008).
[11]. Tomic, D.: The Benefits and Challenges with Implementation of Internet of Things (IoT) in Manufacturing Industry. Unpublished M.Sc. Thesis, KTH Royal Institute of Technology,Tockholm, Sweden, (2017).
[12]. World Economic Forum: Industrial Internet of Things: Unleashing the Potential of Connected Products and Service. Available online at:http:// www3. weforum.org/docs/WEFUSA IndustrialInternet Report2015.pdf, Accessed on 1st May 2018, (2015).
[13]. Yagoob, I., Ahmed, E., Hashen, I.A.T., Gani, A., Imran, M., Guizani, M.: Internet of Things Architecture: RecentAdvances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Connection, vol. 24(3), PP. 10-16 (2017).

Iwayemi A., " Internet of Things: Implementation Challenges in Nigeria"American Journal of Engineering Research (AJER), vol.7, no.12, 2018,pp.105-115