International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 9 Issue 4 April - 2025, Pages: 148-156

Analysis Of Iot Challenges In Nigerian Tertiary Institutions: Solutions And Way Forward

Abubakar Balarabe1, Naseer Sanni Ajoge (PhD)2, Muhammad Muktar Tambuwal3

Faculty of Computing, Department of Computer Science, Mewar International University, Nigeria. Masaka, Nasarawa State Nigeria.
balarabe@miu.edu.ng
College of Science and Technology, Department of Computer Science, Kaduna Polytechnic, Kaduna
ajogenass@kadunapolytechnic.edu.ng
College of Science and Technology, Department of Computer Science, Kaduna Polytechnic, Kaduna
m.tambuwal@kadunapolytechnic.edu.ng

Abstract: *This research analyzed the challenges and solutions of IoT in Nigerian tertiary institution. IoT is an evolving technology and expected to bring the next phase of revolution in learning by connecting any device anywhere by any available means and by collaborating learners and instructors. The potential of IoT applications is abundant, allowing its users to have real-time feeds from surrounding and distant objects helping in making intelligent decisions. Despite the potential benefits of IoT, there are several challenges that needs to be address for IoT to harvest its potential benefits. This paper discussed recent challenges and proposes some solutions concerning IoT. A systematic review of the latest literature covering IoT and some distinct categories of challenges were extracted including standardization and harmonization, connectivity, power management, security, privacy, evolving scenarios, socio-ethical considerations, network technology, complexity, and rapid evolution. Further, the research discusses the latest solutions evolved ranging from flexible radio standards, wireless sensor networks, wireless battery charging technology, ipv6/6lowpan protocols, privacy broker techniques, flexible IP protocol, to wireless identification and sensing platforms.*

Keywords— Internet of Things (IOT), IoT in education, Nigerian tertiary institutions, Higher education Nigeria, IoT challenges, IoT infrastructure, IoT implementation

1. INTRODUCTION

Back in 1989, there were around 100,000 hosts connected to the Internet, and the World Wide Web (WWW) came to life a year later at CERN with the first and only site at the time. Ten years after Tim Berners-Lee unleashed the WWW, a whole new world of possibilities started to emerge when Kevin Ashton, from the Massachusetts Institute of Technology's (MIT) Auto-ID Labs, coined the term Internet of Things (Ashton, 2009). In the same year, Neil Gershenfeld published his work on things that think, where he envisioned the evolution of the WWW as "things start to use the Net so that people don't need to". Simultaneously, in Xerox PARC Laboratories in Palo Alto, California, the so-called third era of modern computing was dawning, with Mark Weiser introducing the concept of "ubiquitous computing" in his paper published in Scientific American (Weiser, 1991). Tabs, pads, and boards were proposed as the essential building blocks for the computing of the future. Wireless networking and seamless access to shared resources would make user experience with technology as enjoyable as "a walk in the woods" (Qusay et al., 2018).

The Internet of Things encapsulates a vision of a world in which billions of objects with embedded intelligence, communication means, and sensing and actuation capabilities will connect over IP (Internet Protocol) networks (Simone et al., 2019).

With a massive number of devices connected to the Internet and the huge data associated with it, there remain concerns about the security. By security it means the degree of resistance to, or protection of the IoT infrastructure and applications. Many of these devices are easy targets for intrusion because they rely on very few outside resources and are often left unattended. Once the network layer is compromised, it is very easy for a hacker to gain control and maliciously use a device as well as attack other devices nearby through the original compromised node. In particular, appliances that maintain an online presence are easy to attack. These devices that do not have any virus protection or malware protection are highly susceptible to being used as "bots" to forward malicious code to infect other devices (Xu, 2013).

The International Data Corporation predicts that more than 200 million devices will be connected to the Internet by the year 2020, with a good amount of these being appliances; there will be a large opportunity for hackers to use these devices to their advantage through "denial of service" attacks, malicious email, and other harmful worms or Trojans. A

HP study reveals that 70% of Internet of Things devices are vulnerable to attacks. As per recent test conducted by HP, about 90% of tested devices collected at least one piece of personal information via the product itself, the cloud or its mobile application (HP 2021). This personal information might easily get compromised due to a cyber-attack or unauthorized access. This will reduce confidentiality, integrity and security of the data and evidently users will be reluctant to adopt this technology. Therefore, a major concern in adopting

and implementing this new technology is security and privacy. Security for the users should be ensured by preventing unauthorized identification and access. By privacy we mean that the data of the user is under his or her own control and no one else. With a very high dependence on the data and devices based on IoT, another issue that arises is reliability. By reliability we mean that the devices need to work effectively, as intended at all times without failure. In addition to the IoT, the data transmitted between the devices and the Internet should be reliable, since giving false information or providing unreliable data is a grave concern as this might lead to taking unnecessary or wrong consequences (Arun et al., 2013).

Equipment are becoming more digitized and more connected, establishing networks between machines, humans, and the Internet, leading to the creation of new ecosystems that enable higher productivity, better energy efficiency, and higher profitability. Sensors help to recognize the state of things, by which they gain the advantage of anticipating human needs based on the information collected per context. These intelligent devices not only gather information from their environment but are also capable of taking decisions without human intervention. IoT technology is being used in our day-to-day life for unlocking the door without a key; in card recognizers, automatic locks, vehicle detecting systems, toll payment system; and for tracking animals, access control, payment systems, contactless smart cards, anti-theft devices, steering column reader, etc. will come from those that are web-enabled devices, providing common platforms on which they can communicate, and develop new applications to capture new users (Tripathy & Anuradha, 2018).

In 1999, the number of hosts exceeded two million and the number of sites jumped to 4 million (Zakon, 2016). The Institute of Electrical and Electronics Engineers (IEEE) standard 802.11b (Wi-Fi) had just been published, with transmission rates of 11 Mbits/s. GSM was growing fast, but the phones were not at all smart yet. They (only) allowed for making phone calls and sending short messages. GPS signals for civil usage were still degraded with selective availability, and the receivers were heavy, huge, and expensive. The area of wireless sensor networks (WSNs) also emerged in the 1990s with the concept of smart dust, a big number of tiny devices scattered around an area capable of sensing, recording, and communicating sensed data wirelessly (Sajad et al., 2018).

All kinds of physical, mechanical, electrical, and electronic objects are thereby instrumented and interconnected with others in the vicinity as well as with remotely held software applications and datasets. With the addition of a bevy of devices (for smarter homes, smarter buildings, and smarter everything), the number of software services getting developed and deployed in central application repositories is growing rapidly. In short, by this year 2020, there will be billions of software applications and trillions of connected devices and digitized entities on this planet. The possible impacts are really mesmerizing for consumers and organizations, let alone for technologists. To us, this is no longer science fiction because it is truly the art of the impossible. The implications, impact, and imperative of this trend are truly irreversible, and the momentum is truly nuclear (Pethuru & Anupama, 2017).

Now that the IoT is finally becoming a reality, there is a need for a global understanding on its definition, applications, Challenges and Solution.

The internet has deeply rooted itself into our schools, and e-learning is becoming common practice in the Nigerian Educational System. With the rapid increase in numbers of Things (devices) other than standard products such as computers and smartphone being connected to the internet every day, the application of the IoT in the education system is in practice, and the implications for this disruption are tremendous which raises questions about security, privacy and cloud attacks.

Implementing a well-secured IoT solutions for education requires the significant power of hardware and software, collecting and processing various forms of digital data will put educational institutions on the map for hacking threats. Before deploying an IoT solution, project stakeholders need to build a contingency plan for data breaches, security attacks, and other threats. Increasing awareness regarding the importance of data security among students and staff is an essential part of the innovation implementation process. This research analyses Problems and Solutions of Internet of Things in Nigerian Educational System.

The aim of this research is to carry out statistical analysis on Internet of Things, analyze the challenges and solutions in Nigerian tertiary institutions. With the sole objectives of identifying the IoT Challenges in Nigeria tertiary institutions. Then analyze the current solutions for these challenges using a questionnaire. And perform statistical analysis and results collections. The study also intended to carry out a comprehensive research on IoT challenges such as privacy, cloud attacks and security issues as it is a serious problem that creates other problems for schools, individuals, organizations and society. Security requires much and better attention in finding solutions that will enhance the security problems.

Never the less, this work is limited to analysis on sample gathered from Tertiary Institutions in Nigeria.

2. LITERATURE REVIEW

2.1 Review of Related Literatures

Ma et al. (2011) conducted a research on library management system based on IoT and proposed library management system of study room seating and library resource utilization based on IoT technology.

Hua and Yang (2012) conducted a research Item Positioning System IPS and designed a personal item positioning system and remote monitoring management system using RFID technology that can be extended and use in libraries.

Renold and Rani (2013) performed a research on IoT in Library that lead them to designed a system with RFID technology for the use of library management, the system includes perception layer, network layer and service layer, can identify the problems in the library, such as the library materials selection, stock management, misplace books and materials, mis-shelved, stack maintenance, etc., promote easy access to the books, articles, journals, etc. and form an internet-based application for library management.

Liu and Yuan (2013) reviewed the literature of IoT technology in libraries, and introduced IoT application and research trends. Discussed smart campus role in digital resources sharing, library management, campus card and information system integration, and proposed the campus model, intelligent services and management based on IoT.

Chen (2013) introduced RFID application in university libraries, and proposed intelligent reservation bookshelf in the intelligent library. Discussed the system of smart library based on RFID, cloud service, data process, privacy protection and standardization. Reviewed the development of library from traditional library to automated library to digital library and to smart (intelligent) library.

van de Pas (2014) analyzed the future of libraries in the internet era, and proposed that the virtual library can provide information services with internet-based services and free access to information.

Yao and Song (2014) designed a library intelligent lighting energy-saving control system based on IoT. They introduced library data information resources and the integration of library information resources in a digital way, and proposed library data resource object model and the process of library personalized information service management.

Grama (2014) investigated the number of reported data breach in the United States in education, and particularly higher education, is often identified as having a large number of reported data breaches, and at first look, the Privacy Rights Clearinghouse database appears to confirm this view. In the United States, there were 727 reported breaches in educational institutions between the years 2005–2014. This number is the second-highest among seven sectors that were investigated (the first is health care). About 7% of all academic institutions in the United States have had a least one breach. From 2005 to 2014, 66% of academic institutions listed in the Privacy Rights Clearinghouse experienced only one reported breach.

Chiu et al. 2014 developed a "Mobile Library APP System," and discussed the mobile application service in library management. Their research leads Li et al. (2016) to the development of an IoT system for library materials management.

Putjorn et al. (2015) discussed particularly the challenge of child privacy when using IoT for education. It has become increasingly clear that educational systems are vulnerable to cyberattacks, and the number of attacks are predicted to increase. Students can easily stage cyberattacks on their institutions, or schools/universities could be prevented from functioning as intended. Cascade failures may appear, caused by the interconnectivity of a large number of devices, difficult to be simultaneously protected over the air transmission, with all the related problems.

Jagtap et al. (2016) addressed the issue of scalability in the context of providing personalized content to the students based on analyzing a large volume of collected student data and activity. They proposed a design for a "social recommender" system that is based on Hadoop and its parallel computing platform.

Chen et al. (2016) discussed shared project data, and annotate learning materials in a real-time and access the learning resources remotely (e.g., remote labs). Findings shows that IoT could also provide support to students with adapted learning resources by integrating content that is based on location, time, date, student-to-student interaction, knowledge level, and so forth.

Lenz et al. (2016) discussed Dehumanization of humans in interacting with machines is a valid concern, their findings shows that face-to-face interaction between students will not only benefit a child's social skills but also positively contribute towards the character building. The issue that may arise from increased IoT technologies in education is the partial loss of the social aspect of going to school. Using IoT in virtual learning environments can be of a special support to students of special needs, e.g., dyslexic and dyscalculic needs. IoT can offer students with special needs the opportunity to randomly often repeat experiments without major damage to property or cost. For dyslexic and dyscalculic students, for example, it is likely that anonymization will be advantageous for them as possible functions because of IoT (e.g., autocorrect) will improve any bias with a student's score because teachers will not know if they are assessing students with a learning challenge or not.

Maki et al. (2016) research introduced diversification on the interfaces of IoT operating systems and library symbol diversification method and explored a security approach for IoT operating systems based on memory layout shuffling and symbol diversification. They proposed optimizing libraries within the Robot Operating System by deploying robotic sensor-actuators in a simulation environment for runtime optimization, which could open up a wide range of use-cases in mobile IoT deployments.

Lee and Yun (2017) designed a system of Noise Information Storage based on IoT. The system can sense raw noise with IoT devices, transmitting noise data from IoT devices to a server, processing the noise data at the server and storing the processed data in a database. The data can be used for restraining the issues and addressing noise sources.

Laplante (2017) identified the challenges of Incorporating IoT in education. When specifying the functionality for IoT education applications, attention is often focused on concerns

such as fitness of purpose, big data, and interoperability. Conventional requirement elicitation techniques such as quality function deployment, joint application development, and domain analysis are usually adequate for these types of requirements. But in IoT applications for education, specific quality requirements are probably of greater concern. Laplante identified three major qualities from the extracted scenarios that may pose a challenge for IoT in education: security, scalability, and humanization.

Galvao et al. (2017) proposed a new energy model in managing public building energy use to enhance the sustainability of library, through the retrofit of the current energy system, based on the concept of the IoT in smart cities. This model consists of a mix of energy generation processes based on photovoltaic panels and biomass boilers.

Mehmood et al (2017) discussed the scalability concern when designing a learning management system. With scalability, concerns regarding the discussion on the cost of the IoT technology in education become also significant. Their research raises a question whether in the long-run IoT devices and Big Data analysis will increase the already existing divide into a two-class learning system: those who can disburse these technologies and those who cannot! At the same time, if going to school should be affordable for everyone, how will schools be able to buy and service IoT devices?

2.2 Research Gap

The literature review has presented insights into where, how and what research has been conducted and made it possible to identify the gaps.

Many proposed solutions must intimately involve humans in the process. Some solutions deploy access control methods, or privacy-awareness applications. For example, in (Ukil,2015), the study proposed the Dynamic Privacy Analyzer (DPA), a solution to make the smart smart meter data owner aware of the privacy risks of sharing smart meter data with third parties. On the other hand, almost half of the proposed solutions suggested taking the human out of the loop. These proposed using cryptographic techniques and information manipulation, or data minimization, to prevent data being sniffed en route to servers. In Tan (2014), an original scheme called the Path Extension Method (PEM) was presented, which provides powerful protection of source-location privacy, by using an encryption technique that ensures an adversary will not be able to eavesdrop on communications. The overwhelming majority of the researchers were fundamentalist about privacy. This is, perhaps, to be expected since unconcerned researchers would not have little interest in carrying out research in this area. It does mean, however, that they might be somewhat unrealistic about the man and woman in the street, and their privacy stance. Unconcerned consumers are likely to be unwilling to take any action at all to preserve a privacy they don't care about. Solutions seem to be designed under the assumption that consumers will naturally be willing to spend time and effort engaging with them. This assumption might well be flawed. The question that demands investigation is whether consumers of various privacy stances would indeed be willing to expend effort to interact with privacy-preserving applications. Researchers are coming up with innovative solutions, but this will be futile in the face of consumer complacency or unwillingness to engage with them.

From the reviewed studies, it can be seen that many areas of IoT application in Nigeria have been discussed. No work was done on the analysis of internet of things IoT, challenges and solutions in Nigerian. This research is going to breach this gap by analyzing the Internet of things, challenges and solutions in Nigerian educational system. IoT is in its newest age in Nigerian Educational System even though the problems and solutions may not be different from the one faced already in other sectors; like Smart Home, Smart grid, Health and Agriculture.

3. RESEARCH DESIGN

A survey design is use for the purpose of this research because it is suitable for the study in dealing with large population. Sequence of Bio-data background of the respondents and multiple-choice questions on analysis of internet of things challenges and solutions in Nigerian educational system. The survey was hosted online. Quantitative method of analysis was appropriately used in the data analysis. Appropriate statistical tools were also applied for interpretations.

The primary data was collected through the use of questionnaire for data analysis. The questionnaire was design online using Google Forms and hard copies was also printed and distributed. The online questionnaire link was distributed via WhatsApp, Email list and Facebook friends list account of Hamza Umar to be accessed by the respondents mostly students and graduates from various universities and colleges in Nigeria.

The data collection techniques used in this research is questionnaire survey technique. The questionnaire was deployed both online and hard copies was distributed to the respondents. The online deployment was included because of speed and flexibility which make survey faster to deploy, and access to wider coverage and a high percentage of respondents.

The research methodology is enumerated as follows:

1.Data gathering from the survey
2. Interpretation of the data
3.Discussion and Validation.

Quota sampling was used for this research. Quota sampling is a sampling method of gathering representative data from a group. Quota sampling requires that representative individuals are chosen out of a specific subgroup. It aims to make the sample representative of the population by setting quota controls or predetermined specification. This type of sampling is used to ensure that specific elements will be included. This technique was used because it is most frequently used in social survey, and it is a quicker and cheaper method.

The method of data analysis to used in this research is that the data will be collected from the instrument, and the scores obtained will be analyzed and help in making decisions using mean and standard deviation to analyze the collected research questions data from the questionnaire distributed to the students and graduates.

4. Data Presentation and Analysis

From the survey responses gathered, a total of 96 (100%) respondents responded to the survey, 55% are students while 45% are graduates from various institutions within Nigeria. This implies that the number of responses received with respect to the research which was conducted on the subject matter as it relates to the Internet of Things in Nigeria Educational System is valid because 100% of the total responses is applicable. This is shown in the Table 1.

Table 1: Response from Institutions

University/College	Respondents	Percentage (%)
Abubakar Tafawa Balewa University, Bauchi	2	2.1%
Ahmadu Bello University, Zaria	12	12.5%
Bayero University, Kano	10	10.4%
Bayero University, Kano, Kano	2	2.1%
Hassan Usman Katsina Polytechnic	2	2.1%
IMO State University	2	2.1%
Kaduna Polytechnic, Kaduna	22	22.9%
Kaduna State University, Kaduna	10	10.4%
National Teachers' Institute, Kaduna	4	4.2%
Niger State College of Education Minna	2	2.1%
Nigerian Defence Academy PGS	20	20.8%
Nuhu Bamalli Polytechnic, Zaria	2	2.1%
Usmanu Danfodio University, Sokoto	6	6.3%
Total	**96**	**100.0%**

4.1 Educational Level of Respondents

Table 2 and Figure 2 shows the educational background of respondents. Table 2 and Figure 2 shows the distribution of respondents, 38 (40%) are undergraduate with the highest percentage in the survey, 34 (35%) are postgraduate and 24 (25%) graduate.

Table 2: Respondents by Educational Level

Educational Level	Respondents	Percentage (%)
Undergraduate	38	39.6%
Graduate	24	25.0%
Postgraduate	34	35.4%
Total	**96**	**100.0%**

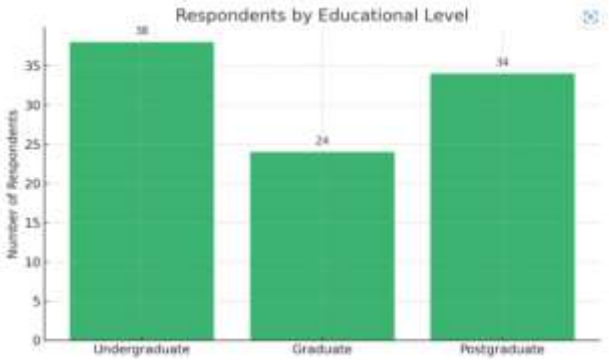

Figure 2: Respondents by Educational Level

4.2 Distribution of IoT

1. Uses in Nigerian Institutions

Table 3 shows the scale from 1 to 5 level of how Nigerian institutions uses IoT. The respondents show that IoT is being used in a scale of 3 with 52 (54.2%), this implies that most of the institution are halfway of the application of IoT in academic activities.

Table 3: Distribution showing Application of IoT Nigerian Educational System

Scale	Respondents	Percentage (%)
1	12	12.5%
2	16	16.7%
3	52	54.2%
4	8	8.3%
5	8	8.3%
Total	**96**	**100.0%**

2. Distribution showing IoT Provides Smart Learning and Improving the Quality of Learning

Table 4 and Figure 3 shows that IoT provides a smart environment for learning and supports learning and improves the quality of education in Nigerian institutions. It shows that 46 (47%) Strongly agree while 44(45%) agree with IoT is improving the quality of education in Nigerian institutions.

Table 4: Distribution showing IoT Provides Smart Learning and Improving the Quality of Learning

Option	Respondents	Percentage (%)
Strongly disagree	2	2.1%
Disagree	2	2.1%
Neutral	2	2.1%
Agree	44	45.8%
Strongly agree	46	47.9%
Total	**96**	**100.0%**

International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 9 Issue 4 April - 2025, Pages: 148-156

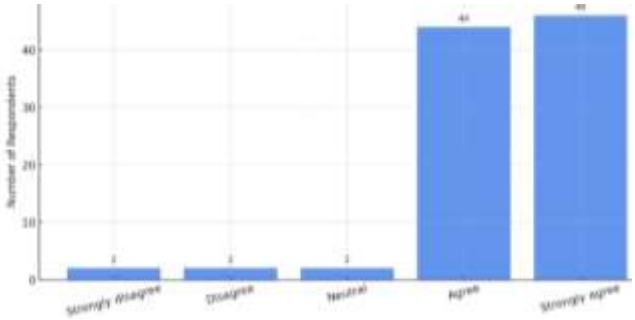

Figure 3: Percentage showing IoT is improving the quality of learning

3. Will deploying access control methods, or privacy-awareness applications help in protection IoT from attack?

Table 5 shows that 40 (41%) respondents strongly agree and 50 (52%) agree that access control methods and privacy awareness will protect IoT from attacks.

Table 5: Distributions of Respondents showing access control methods and privacy awareness will protect IoT from attack

Option	Respondents	Percentage (%)
Strongly Disagree	1	1.1
Disagree	3	3.1
Neutral	2	2.1
Agree	50	52.1
Strongly Agree	40	41.7
Total	**96**	**100.0**

4. Is IoT important in Nigerian institutions?

Table 6 and Figure 4 shows that 92 (95%) agree IoT is very important in Nigerian education, only 4% disagree in its importance in the Nigeria tertiary institutions.

Table 6: Distributions showing importance of IoT in Nigerian educational system.

Option	Respondents	Percentage (%)
Yes	92	95.8%
No	4	4.2%
Total	**96**	**100.0%**

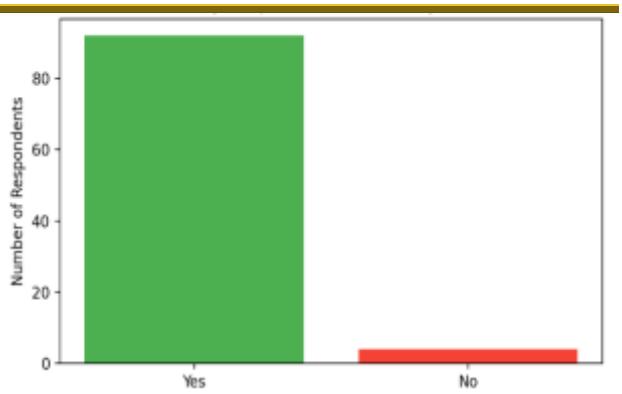

Figure 4: Percentage showing importance of IoT in Nigerian tertiary institutions

5. What are the challenges that affects Internet of Things in Nigeria higher institutions?

Respondents were asked to choose at least 3 from the questions, options include general IoT challenges (Standardization, Connectivity, Electricity, Security, Privacy, Complexity, Rapid Evolution and Network).

Table 7 and Figure 5 shows that standardization (interoperability and Harmonization) are one of the major problems of IoT in Nigerian higher institutions. 52 (54%) Strongly agree and 6 (6.3%) agree respondents agree to that.

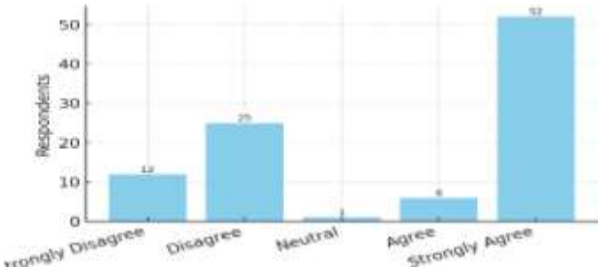

Table 7: Distributions of Standardization as a problem to IoT

Option	Respondents	Percentage (%)
Strongly Disagree	12	12.5
Disagree	25	26.0
Neutral	1	1.1
Agree	6	6.3
Strongly Agree	52	54.2
Total	**96**	**100.0**

Figure 5: Percentage showing importance of IoT in Nigerian tertiary institutions

Table 8 shows that 47 (49%) and 8 (8%) respondents agree that connectivity is one of the challenges facing IoT in Nigerian institutions.

Table 8: Distributions of Connectivity as a Problem to IoT

Option	Respondents	Percentage (%)

Strongly Disagree	13	13.5
Disagree	26	27.1
Neutral	2	2.1
Agree	8	8.3
Strongly Agree	47	49.0
Total	**96**	**100.0**

5. CHALLENGES AND SOLUTIONS

Any new technology faces a lot of challenges till it matures and put to use. IoT, which involves seamless working of anything situated anywhere, and communicating using the Internet, faces many challenges that are worth highlighting. Some of the key challenges facing the Internet of thing in general have been extracted in detail.

Standardization is one of the key pre-requisites of a successful technology development because it creates interoperability among devices that are manufactured by different vendors, suppliers, and countries which allows the technology to gain commonality and popularity among users. Since IoT operates with multiple devices, it makes sense to have common standards among these devices to operate together and to gain market popularity. For instance, the popularity of mobile phone is attributed to standards such as GSM, TCP/IP, IMT-2000 etc.

A collaborative effort is ongoing at the level of ITU-T Study Group 20 meant for standardization of IoT and Smart Cities and Smart Communities, Nigeria should key into this. Also, cross-sectorial collaboration would go a long way in improving the situation since IoT is developed in different sectors and sharing ideas across sectors would improve the Standardization and Regulatory issues (Kunle, 2017).

Although the potential of IoT in connecting anything anywhere is promising, it adds a key challenge with regards to IoT devices connectivity. The devices can be stationary or moving and may use several types of technology for communication. Thus, the system cannot use a single connectivity solution. Rather, wide varieties of wired and wireless standards will be involved to provide connectivity. A real challenge will be to make different standards communicate with one another seamlessly to establish the targeted connectivity (Chase, 2013).

One of the key technologies to be used for connecting various devices in IoT is Wireless Sensor Network (WSN). However, when used for IoT, the WSN is also be connected to the Internet. The challenge for existing scheme proposed to provide security in WSN must provide security from Internet as well. The device heterogeneity in IoT also requires special techniques for workload distribution in WSN to maintain system quality of service. The sheer volume of devices using WSN may undergo a revamp of current protocols to handle these volumes and traffic. Further, the nodes in WSN may also need management of their configuration settings (Chase, 2013).

Similar to current health tracking tools on mobile phones or watches, IoT devices can avail significant amount of personal data on IoT users' location and movements, health conditions, and purchasing preferences. This can invade personal privacy for individuals using IoT technology. Although IoT service providers may seek to protect personal privacy, they are sacrificing a massive data that can improve the quality of people's lives and decreasing service providers' costs by streamlining operations. In spite of the overall benefits for the general public, individuals still prefer to protect their own privacy even it means sacrificing the overall public benefit. According to the 2014 eTRUST Internet of Things Privacy Index, only 22% of Internet users agreed that the benefits of smart devices outweighed any privacy concerns. While the IoT continues to gain popularity through smart home technology and wearable devices, confidence in and acceptance of the IoT will depend on the protection of users' privacy.

Whatever the solution for privacy is, it has to conceal personal information and control what happens with the information collected. A substantial number of schemes has been proposed for privacy of RFID and can be broadly categorized into two types: schemes that limit physical access and schemes that use passwords. The physical-based scheme uses methods such as deactivate tag, clip tags, block tags, shield tags etc. In most of these schemes, the tag is disabled after its final use. For example, after the user pay for the item, the tag gets automatically disabled to avoid tracking the user. The password-based schemes use encryption and include schemes such as hash chain, noisy tags, anonymous ID etc (Weis et al. 2004).

Providing privacy in areas where sensor networks are deployed is more challenging as the person entering the area has no control over data being collected related to an individual (Atzori et al., 2010). The personal data collected need to be used only by authorized service provider for authorized services. The use of a system called privacy broker has been suggested for this. In this system, a proxy is used that interacts with user who can set the access setting for a service provider. This allows the service provider to access only the data that is authorized for their service. But this system may not scale to IoT requirements. Another solution being considered is the use of a system that allows digital forgetting which means that data get automatically deleted after certain instance (Atzori et al., 2010).

The IoT deployment requires developments in network technology which is essential for IoT to live up to its expected vision to connect to objects and bring them into the Internet. Technology such as RFID, short-range wireless technologies and sensor networks are enabling this, while for example IPv6, with its expanded address space, allow that all objects or things to be connected, and be tracked. To make this possible, the network technology must be affordable and viable to connect all these devices together. Further, since protocol gateways translation can be complicated for such devices, current IP

solutions provides end to end communication between these devices without intermediate protocol. New scalable architectures designed specifically for the ubiquitous sensor networks communications would allow for networks of billions of devices. Improvements in techniques for secure and reliable wireless communication protocols would also enable mission-critical applications for ubiquitous sensor networks based on wireless identifiable devices (Miorandi, 2012).

6. Conclusion

The research was successfully conducted and results validated. In IoT the seamless interconnection and communication between billions of devices is a challenging task. Handling of sheer volume of devices itself is a challenging task, whether its identification, privacy or networking. The technological challenges include those related to standardization and harmonization, connectivity, power management, security, privacy, complexity, evolving, network technology, complexity, and rapid evolution. Tackling these challenges require the development of a strong framework for each aspect and use of advance technologies that are efficient as well as lightweight. The automation of human activity without human interaction can have serious socio-ethical problems in the educational environment if the IoT technology is not regulated and controlled. The system complexity and constant evolution of device, techniques make IoT a very challenging task and require further research and continuous investigation.

Based on the findings, Security needs much more attention and need to be improve in-network and among IoT devices. The development of algorithm that deleted data in IoT server after certain period of time when not needed will protect user's privacy.

7. References

Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., & Alizadeh, M. (2019). The application of internet of things in healthcare: a systematic literature review and classification. Universal Access in the Information Society, 18(4), 837-869.

Aldeen, Y. A. A. S., & Qureshi, K. N. (2018). New trends in internet of things, applications, challenges, and solutions. Telkomnika, 16(3), 1114-1119.

Aleisa, N., & Renaud, K. (2017, January). Privacy of the Internet of Things: a systematic literature review. In Hawaii International Conference on System Sciences 2017 (pp. 5947-5956).

Ali, F., Khan, M. S., & Akhtar, H. (2019). Security review in internet of things. Internet of Things and Cloud Computing, 7(3), 80.

Ali, M., ElTabakh, M., & Nita-Rotaru, C. (2005). FT-RC4: A robust security mechanism for data stream systems.

Allam, H., & Chaudhri, A. A. (2017). Internet of Things: Extracting Latest Challenges and Solutions. J. Commun., 12(9), 538-542.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

Bagci, I. E., Raza, S., Chung, T., Roedig, U., & Voigt, T. (2013, June). Combined secure storage and communication for the internet of things. In 2013 IEEE International Conference on Sensing, Communications and Networking (SECON) (pp. 523-531). IEEE.

Bedi, G., Venayagamoorthy, G. K., & Singh, R. (2016, March). Navigating the challenges of Internet of Things (IoT) for power and energy systems. In 2016 Clemson University Power Systems Conference (PSC) (pp. 1-5). IEEE.

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: a literature review. International Journal of Production Research, 57(15-16), 4719-4742.

Biggs, P. (Ed.). (2005). ITU Internet reports: the Internet of things. International Telecommunication Union.

Bouzembrak, Y., Klüche, M., Gavai, A., & Marvin, H. J. (2019). Internet of Things in food safety: Literature review and a bibliometric analysis. Trends in Food Science & Technology, 94, 54-64.

Chase, J. (2013). The evolution of the Internet of things, Texas Instrum. Dallas, TX, USA, White Paper, 7.

Christin, D., Reinhardt, A., Mogre, P. S., & Steinmetz, R. (2009). Wireless sensor networks and the internet of things: selected challenges. Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose sensornetze, 31-34.

Cirani, S., Ferrari, G., Picone, M., & Veltri, L. (2018). Internet of Things: Architectures, Protocols and Standards. John Wiley & Sons.

Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A., & Satapathy, S. C. (Eds.). (2018). Internet of things and big data analytics toward next-generation intelligence (Vol. 35). Berlin:: Springer.

E. Trust. (2014). Internet of things privacy index-US. Trust. Retrieved July, 2021, from http://www.truste.com/resources/

HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 100129.

Hassan, Q. F., & Madani, S. A. (Eds.). (2017). Internet of things: Challenges, advances, and applications. CRC Press.

HP Whitepaper. retrieved July 2021 from http://go.saas.hp.com/fod/internet-of-things

Hu, F. (2016). Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations. CRC Press.

Hussain, M. I. (2017). Internet of Things: challenges and research opportunities. CSI transactions on ICT, 5(1), 87-95.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

Kanuparthi, A., Karri, R., & Addepalli, S. (2013, November). Hardware and embedded security in the context of internet of things. In Proceedings of the 2013 ACM workshop on Security, Privacy & dependability for cyber vehicles (pp. 61-64).

Kassab, M., DeFranco, J., & Laplante, P. (2020). A systematic literature review on Internet of things in education: Benefits and challenges. Journal of Computer Assisted Learning, 36(2), 115-127.

Kopetz, H. (2011). Real-time systems: design principles for distributed embedded applications. Springer Science & Business Media.

Koroniotis, N., Moustafa, N., & Sitnikova, E. (2019). Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions. IEEE Access, 7, 61764-61785.

Kumar, N. H., & Prabhudeva, S. (2021, April). SBAP: A Novel Secure Bucket Access Protocol for Leveraging User's Data Privacy in Cloud Environment. In Computer Science On-line Conference (pp. 37-46). Springer, Cham.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5772-5781). IEEE.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5772-5781). IEEE.

Kunle, O. J., Olubunmi, O. A., & Sani, S. (2017, November). Internet of things prospect in Nigeria: Challenges and solutions. In 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON) (pp. 736-745). IEEE.

Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals.

Liang, X. (2018). Internet of Things and its applications in libraries: a literature review. Library Hi-Tech.

Liao, Y., Loures, E. D. F. R., & Deschamps, F. (2018). Industrial Internet of Things: A systematic literature review and insights. IEEE Internet of Things Journal, 5(6), 4515-4525.

Lynggaard, P. (2014). Artificial intelligence and Internet of Things in a "smart home" context: A Distributed System Architecture.

Maxwell, G. S. (2021). Looking Back and Looking Forward. In Using Data to Improve Student Learning (pp. 373-397). Springer, Cham.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), 1497-1516.

Mukhopadhyay, S. C., & Suryadevara, N. K. (2014). Internet of Things: Challenges and Opportunities. Internet of Things: Challenges and Opportunities. Mukhopadhyay (pp. 1–17). Heidelberg, SC.

Ni, J., Zhang, K., Lin, X., & Shen, X. (2017). Securing fog computing for internet of things applications: Challenges and solutions. IEEE Communications Surveys & Tutorials, 20(1), 601-628.

Palmaccio, M., Dicuonzo, G., & Belyaeva, Z. S. (2020). The internet of things and corporate business models: A systematic literature review. Journal of Business Research.

Pico-Valencia, P., & Holgado-Terriza, J. A. (2018). Identification of the Internet of Things: A systematic literature review. International Journal of Distributed Sensor Networks, 14(10), 1550147718805945.

Qureshi, K. N., & Abdullah, A. H. (2014). Localization-based system challenges in vehicular ad hoc networks: survey. smarter, 4(6), 515-528.

Radu, L. D. (2018). Environmental Issues in Internet of Things: Challenges and Solutions. Acta Universitatis Danubius. Œconomica, 14(1), 20-32.

Raj, P., & Raman, A. C. (2017). The Internet of Things: Enabling technologies, platforms, and use cases. CRC Press.

Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454-1464.

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. Cluster of European research projects on the internet of things, European Commission, 3(3), 34-36.

Vashi, D., & Patel, V. (2017). Security, privacy and trust issues in internet of things. International Journal of Innovations & Advancement in Computer Science.

Vatsa, V. R., & Singh, G. (2015). A literature review on internet of things (IoT). International Journal of Computer Systems, 2(8), 355-358.