University of Ibadan
Journal of Science and Logics in ICT Research

Towards SDG-9: An IoT Architecture for Converging OT-IT in Industry 4.0 and Digital Economy Era

[1]Abass, Olalere. A., [2]Dawodu, Adekunle A. and [3]Yisau, Nurudeen B.

[1,3]Dept. of Computer Sc., Tai Solarin College of Education, Omu-Ijebu, Ogun State.
[2]Dept. of Computer Science, D.S. Adegbenro ICT Polytechnic, Ogun State, Nigeria,
olaabas@gmail.com; alandawodu@gmail.com; yisautunde@gmail.com

Abstract

The Internet of Things (IoT) has the capacity to change the world in similar way as Internet. IoT is a technology that has potential to change the industry landscape by connecting smart devices. In the current era of cheap computing resources, unlimited bandwidth and 24/7 internet-based connection of devices, the adoption of IoT by the developing countries like Nigeria has the prospect of improving all sectors of economy like agriculture, industry, health etc. The target of the technology is to impart on the companies' competitiveness and betterment of citizens' quality of life but security of the technology remains a challenge. Hence, this paper focuses on the development of a security-enhanced architecture that merges the two main components of IoT (information technology and operation technology) towards achieving the 9th Sustainable Development Goal (SDG-9) as formulated by the United Nation. The paper shows that to achieve SDG-9 in the digital economy era of Industry 4.0, adequate attention should be paid to the implementation of IoT secured architecture by the developing countries. The paper concludes by identyfing two major factors (technical and funding) that serve as barriers to achieving SDG-9 and subsequently proffer solutions.

Keywords: *Internet-of-Things, IoT devices, Gateway, Digital economy, SDG-9*

1. INTRODUCTION

In September 2015, the United Nations at its General Assembly in New York agreed on a new global 17-point partnership development plan tagged "Sustainable Development Goals" (SDGs) to be achieved by the year 2030. The Ninth SDG (SDG-9) was named "Industry, Innovation and Infrastructure" with a broad objective of building resilient infrastructure, promote all inclusive industrialization and foster innovation. The objective is based on the great recognition that utilization of information and communication technology (ICT) is the major determinant of achieving SDGs because the technology plays a critical role in transforming societies and economies by enhancing efficiency, connectivity and access to resources and services" [1]. According to Sachs [2], these SDGs offer a lead way to ending poverty, fight inequality and tackle climate change. Sach [2] further states that the goals are wide-ranging but have one thing in common and all rely on the enabling power of ICT which is a catalyst that enhances the achievement of all the SDGs in the current era of Industry 4.0 (or Industrial Internet) aimed at fostering digital economy across the globe. Increasingly, varieties of industrial-based organizations are using Internet of Things (IoT) to operate more efficiently, better understand customers towards delivering enhanced customer services, improve decision-making and increase the value of the business [3].

The Industrial IoT (IIoT) and the fourth internet-enhanced industrial revolution (Industry 4.0) are names given to the use of IoT technology in a business setting. Industry 4.0 is geared towards automation and data exchange in manufacturing technologies and processes. Industry 4.0 focuses on having machines which are augmented with wireless connectivity and sensors that are connected to a system capable

ABASS, O. A., DAWODU A. A. and YISAU, N. B. (2021). Towards SDG-9: An IoT Architecture for Converging OT-IT in Industry 4.0 and Digital Economy Era.. *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR),* Vol. 6 No. 2, pp. 57-67

of monitoring the whole production lines and make decisions on their own. Industry 4.0 is fully achieved through technologies such as IoTs, cloud computing, cognitive computing, blockchain technology, robotic process automation and artificial intelligence [4].

Currently, the fast spread of IoT is one of the biggest technology trends taking place in industrial environments. Contrary to the big advances in industrial technology during the past decades, the IoT as a new phenomenon demands intimate collaboration between information technologies (IT) and operational technology (OT). IT means anything related to computer technology including hardware and software. OT is the hardware and software that detects or causes a change through a direct monitoring and control of industrial equipment, assets, processes and events. The major difference between OT and IT devices is that OT devices control the physical world while IT systems manage data. IT handles the information aspects of technological-based industries while OT handles the machinery aspects. Convergence of IT and OT, a necessity in Industry 4.0 era, takes different forms based on firms' unique features, context and goals but its success is hinged on addressing three broad issues which are *data*, *security* and *competencies* [23]. Hence, the motivation of this paper is to develop an architecture that converge IT and OT as well as addressing the contentious and important security issue towards enhancing industrial growth to achieve SDG-9 in the digital economy era.

This paper is organized as follows: Section II focuses on literature review that discusses adoption rate of ICT in Africa towards achieving 9th SGDs, concepts of digital economy, IoT, OT-IT convergence, IIoT and industry 4.0. Section III is on the development of IoT architecture for converging OT-IT. Section IV deals with discussions while Section V concludes the paper.

2. LITERATURE REVIEW

2.1 Related Works

Murray, Johnstone and Valli [24] investigate the state of cyber security in OT and present a demonstration to converge IT and OT using Hofstede's model which focus on organisational acculturation to explain diverse value and attitudes as drivers in IT and OT. The result of the research showed that there exist dividing line in values between the IT and OT technologies and concluded that the variation leads to the difference in significance placed on information security properties (OT availability and IT confidentiality) by each group studied.

Jeff-Meyers [25] studies on the convergence of IT and OT that has the potential to enable the development of Smart Grid technology capable of transforming the operations of utility and passing IT across traditional boundary into OT. The author presents an architecture that shows the dynamic integration of IT and OT. The researcher opines that the merger of these two technologies as utilities can supplement the convergence for smarter, greater cost effective and reliable operations in industrial organizations. It was concluded that the approach of converging IT/OT has the potential to deploy each of the grids for modernization in industrial applications.

However, no literature focused on identifying the components of Industry 4.0 and their interconnection with IT and OT in secured environment using gateway and platform layers. Hence, this paper attempts to address this issue in IoT architecture.

2.2 Adoption Rate of ICTs in Africa for Success of the SDGs

Many African countries now adopt ICTs to achieve SDGs but the diffusion is at a slower rate such that the gap between the information-rich developed countries and Africa remains widen everyday [5]. Consequently, most African countries are yet to reap the abundant benefits of the global information society and the digital economy in areas such as manufacturing, education, health, commerce, agriculture and rural development [6]. Figure 1 shows the important indicators about ICT in Africa during a decade period of 2005 – 2015.

2.3 Digital Economy: Meaning, Components and Benefits

The term 'digital economy' was first coined in a book titled "The Digital Economy: Promise and Peril in the Age of Networked Intelligence" by Don Tapscott in 1995. Digital economy (also known as Web Economy or Internet Economy) is one collective terms for all economic transactions that occur on the internet. With the advent of technology and the process of globalization, the digital and traditional economies are merging into one.

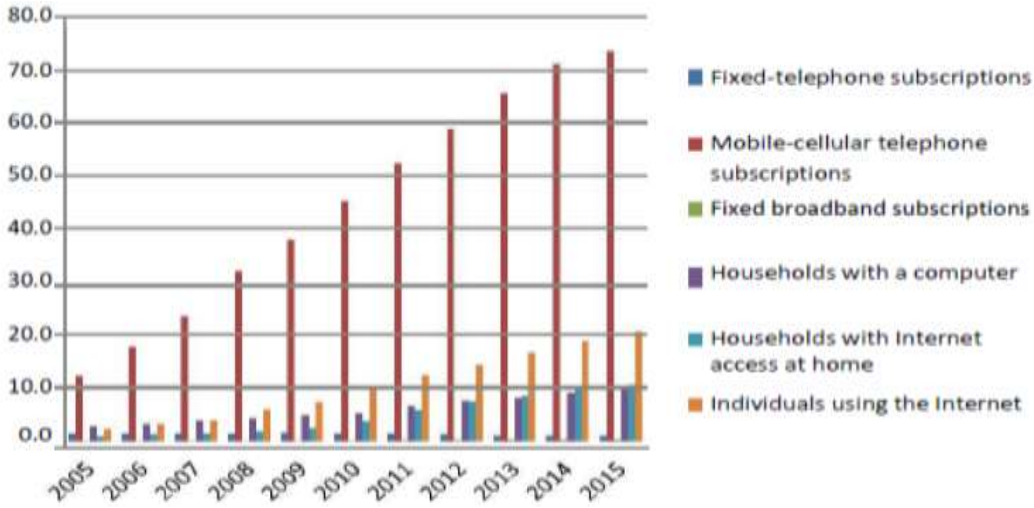

Figure 1: ICT Indicator in Africa [7]

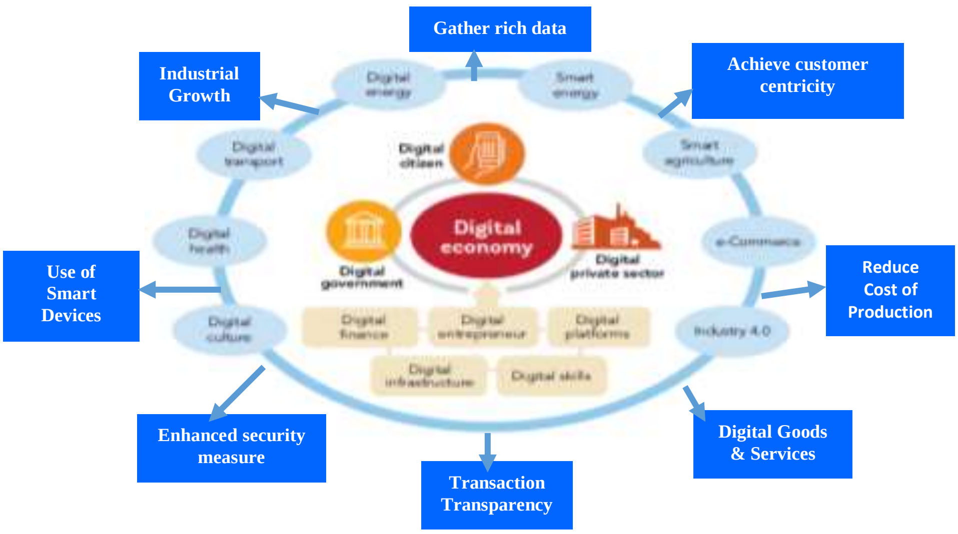

Figure 2: Components and Applications of Digital Economy

Digital economy focuses on digital computing technologies and covers all business, economic, social, cultural etc. activities that are supported by the web and other digital communication technologies as shown in Figure 2.

2.4 Internet of Things Concepts

The IoT has the potential to change the world just as the Internet did [8]. The term was first coined by Ashton with regards to Radio Frequency Identification (RFID) and the Internet with the vision that a computing world will acquire knowledge without human intervention where computers that are enabled with sensing capabilities can understand the world without the limitations of human created data [9]. IoT technology focus on connection of smart devices that have the capability to change the scalable industry landscape. In the era of cheap computing resources, unlimited bandwidth and 24/7 connected devices, the applications of IoT range across all industries from agriculture to space [10].

According to Rayes and Salam [8], IoT presents a future world where all the 'things' in our ambient environment are connected to the Internet and seamlessly communicate with each other to operate intelligently in order to enable devices around us efficiently sense our surroundings, inexpensively communicate, and ultimately create a better environment where such devices act without explicit instructions. The main idea of IoT is to physically connect anything/everything (e.g., sensors, devices, machines, people, animals, trees and processes over the Internet for monitoring and/or control functionality. The IoT services are explored using intelligent interfaces and made available anywhere, anytime, and for anything taking security into consideration [11].

2.5 IoT Components, Requirements and Framework

Generally, IoT is a network of physical elements based on the availability of (a) *Sensors* to collect information, (b) *Identifiers* to identify the source of data like sensors, actuators and other devices, (c) *Software* to analyze data and (d) *Internet connectivity* to communicate and notify users [4]. Rayes and Salam [8] opine that some companies (e.g., Cisco) refer to IoT as the IoE (Internet of Everything) with four key components:

i. *People*: Connecting people in more relevant ways.
ii. *Data*: Converting data into intelligence to make better decisions.
iii. *Process*: Delivering the right information to the right person or machine at the right time.
iv. *Things*: Physical devices and objects connected to the Internet and each other for intelligent decision-making.

There are three basic requirements to monitor and control processes in IoT: (a) uniquely identity per “thing” using Internet Protocol (IP) address, (c) the ability to sense specific information about the thing (sensors) and (c) the ability to communicate between things (e.g. wireless communications), and With these three requirements, users should be able to monitor things from anywhere in the world [12]. In terms of implementation, Figure 3 shows a framework that divides IoT solution into the four major levels [8].

i. Devices Level: Devices make reference to “things”. These include all IoT sensors and actuators.
ii. Network Level: This level focuses on infrastructure transporting the data. The components required are gateways, routers and switches.
iii. Service Platform Level: The level includes the key management software functions to enable the overall management of IoT devices and network. It also includes main functions connecting the device and network levels with the application layer.
iv. IoT Application Level: The level deals with specialized business-based applications like customer relation management (CRM), Accounting and Billing, Business Intelligence (BI).

According to Zaidan and Zaidan [13], control in IoT is passed down from one level to the one below, starting at the application level and proceeding to the devices level and backup the hierarchy. IoT devices make up the physical hardware component of various solutions. In industrial equipment monitoring use-case, these devices are things like engines and their controllers. For smart environment use-cases, these could be motion sensors or badge readers and for asset tracking use-cases, these are GPS. Figure 4 shows typical working environments of IoT. Some examples of IoT-enabled devices are smart mobiles, smart refrigerators, smart watches, smart fire alarm, smart door lock, smart bicycles, medical sensors, fitness trackers, smart security system etc. The technologies used in these devices are low energy wireless and bluetooth, wireless protocols etc.

2.5 Information Technology and Operational Technology

Information Technology (IT) refers to the use of any computers, storage devices, infrastructure and other physical devices to create, process, store, secure and exchange different forms of electronic data. In addition to aforementioned, IT embraces software (such as operating systems, applications), physical servers, networking and other surrounding equipment. There is no limitation to the set of task IT can perform because IT can be re-programmed in different forms in response to the evolving applications, business change requirements and user’s needs. IT networks and manages organizational information which makes the technology a pillar of most organizations and companies.

Operational Technology (OT) refers to technology monitoring and controlling processes and specific devices in an industrial

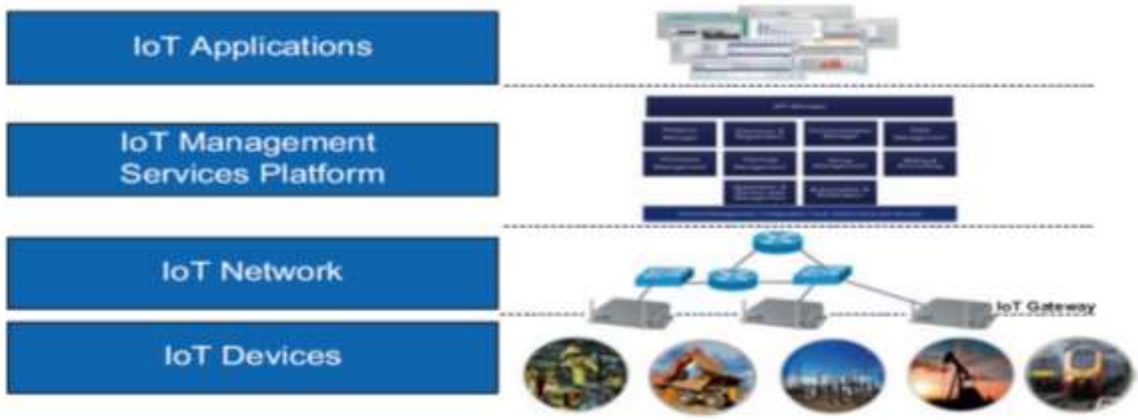

Figure 3: IoT Level [8]

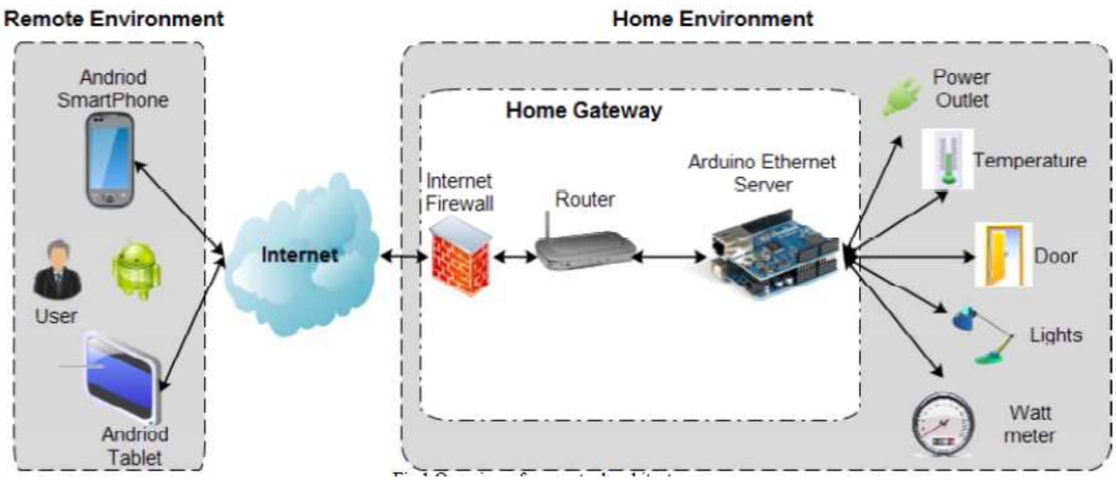

Figure 4: IoT working environment [13]

setting. It combines hardware and software purposely designed to carry out real-time operations. OT devices are not necessarily often updated as they may take months or years to update them. These devices are highly specialized and not designed to run on standard operating systems like iOS and Windows but need customized software to function.

Some of the differences between IT and OT are:

a. IT deals with information while OT deals with machines.
b. IT deals with transactional, voice, video and big data while OT deals with monitoring, control, and supervisory data.
c. IT handles transactional processing of data while OT operates on data in real-time.
d. Data is lost during IT failure while OT network failure may result in death or injury.
e. Frequent upgrade is required in IT network while specific upgrade is done only during the period of specific operational maintenance.
f. Standard operating systems are needed to run IT systems while OT systems run on customized software.

3. IoT: Implementation and IT-OT Convergence

IoT implementation requires tight integration between information technology (IT) and operational technology (OT). Indeed, IT and OT now work together to monitor and regulate essential industrial and business processes beyond regular IT workflows [14].

According to Ibrahim and Huimin [15], IT and OT were, for a long time, regarded as two distinct areas of an organization. Nowadays, these two domains are converging with the rise of connected embedded devices in the IoT and industrial control systems. In IT/OT convergence, there exists integration of OT such as supervisory control and data acquisition

(SCADA), remote terminal unit, programmable logic controllers, and meters and sensors, which work in real time or near real time with IT systems [15]. The IT systems are purposely used for data-centric computing while OT systems are used to monitor events, processes and devices and make adjustments in enterprise and industrial operations [8].

IT-OT convergence is one of the factors driving IoT as depicts in Figure 5. In some firms, the IT and OT are two technologies have never been in agreement, let alone worked together to deploy an IoT system because they have different perspectives on IoT and questions about how to build a collaborative relationship [24]. However, successful industrial/business outcomes (in many cases) hinge on IT/OT convergence.

Bradicich [16] observed that IT and OT convergence can be portioned into three main categories:

i. Process convergence – where IT and OT personnel simply work together.
ii. Data and software convergence – where OT ("things"), data and analytics blend with enterprise data and application stacks.
iii. Physical convergence – where OT systems (control, DAQ and industrial networks) and IT systems (that compute, store and manage data) are physically integrated in a single system.

3.1 IoT Devices

Regardless of use-case, nearly every IoT solution involves the four components: *devices*, *connectivity, platform*, and *software application* (or program). Some use-cases may involve additional layers, but these four components represent the foundation of every IoT solution [17]. IoT involves extending internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects [18]. For example, IoT systems in a high-tech car identifies the traffic ahead and automatically sends out messages to the person the owner is about to meet of his/her impending delay. IoT devices, or many things in the IoT, are nonstandard computing devices that connect wirelessly to a network and have the ability to transmit data. IoT devices which can be connected to input port of an industrial machine include wireless sensors, actuators and computer devices. They are attached to a particular object that operates through the internet, enabling the transfer of data among objects or people automatically without human intervention. A sensor detects physical environment and thereafter responds according to some input received. The input can be in any form like heat, light, pressure, moisture, motion and other environmental factors. The sensor performs some processing on the collected inputs and generates human-readable outputs. Broadly speaking, sensors are devices or machines used to detect the presence of any physical object in the vicinity and send information about the same to the receiving end and the device is mostly used with other electronic devices [10].

Embedded with technology, these new devices (as shown in Figures 6) can communicate and interact over the internet, and they can be remotely monitored and controlled. The networking, communication and connectivity protocols used with internet-enabled devices largely depend on the specific IoT application deployed. Just as there are many different IoT applications, there are also different forms of wireless connectivity protocols which include IPv6, LPWAN, Zigbee, Bluetooth Low Energy, Z-Wave, RFID and NFC. Cellular, satellite, Wi-Fi and Ethernet can also be used. To share the data sensors collect, IoT devices connect to an IoT gateway or another edge device where data can either be analyzed locally or sent to the cloud for analysis [4].

It has been projected that the number of IoT devices will rise from 30.73 billions in the current year to approximately 75.44 billions in 2025 as shown in Figure 7. This means that there will be sporadic increase in the integration of IoT into the industrial revolution for sustainable development.

3.2 IIoT and Industry 4.0

Industry 4.0 refers to the fourth industrial revolution. The term was coined in 2011 to represent the role that cyber-physical systems (CPS), cloud computing, and IIoT will have on manufacturing processes. Industry 4.0 is the era of smart machines, storage systems and production facilities that can autonomously exchange information, trigger actions and

Figure 5: IoT Driving Factors [8]

Figure 6: IoT Driving Factors [8]

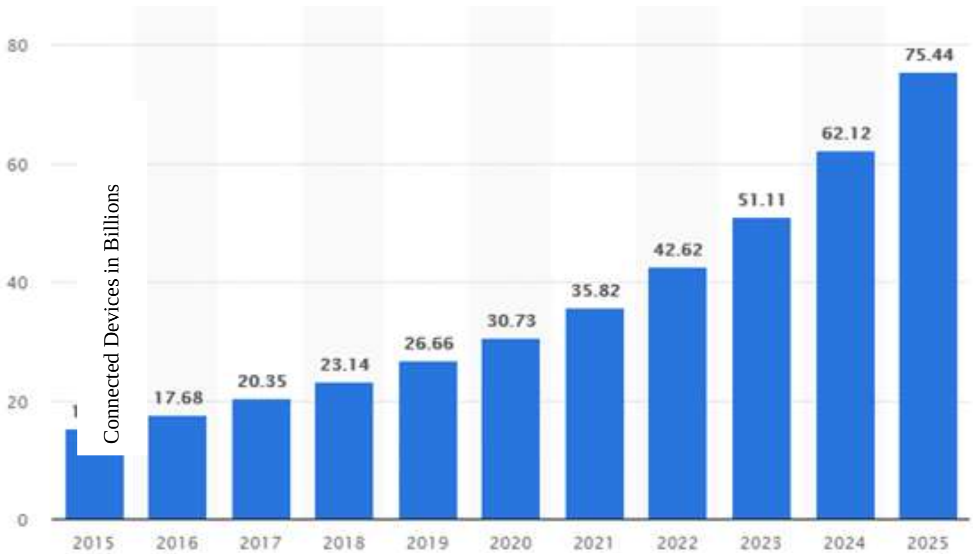

Figure 7: IoT Devices Projection [19]

control each other without human intervention. Currently, the exchange of information is made possible with the IIoT. The impacts of the technology include information decentralization, interoperability of systems, real-time data collection and improved flexibility**.** It also enhances system openness, real-time deterministic control with many core-processors, machine learning (ML), embedded web-based technologies, and other advances are possible by applying IoT technology to industrial operations [20]. As Industry 4.0 and IIoT concepts become real applications, exciting benefits can be achieved by integrating IT and OT. Shea and Haughn [21] opine that large IT companies have promoted ideas like workload consolidation for businesses to optimize processes and be more competitive in their respective industries.

The key elements of Industry 4.0 include:

i. Cyber-physical system: A mechanical device that is run by computer-based algorithms.
ii. The Internet of things (IoT): Interconnected networks of machine devices and vehicles embedded with computerized sensing, scanning and monitoring capabilities.
iii. Cloud computing: This deals with offsite network hosting and data backup.
iv. Cognitive computing: Technological platforms that employ artificial intelligence.

4. IOT ARCHITECTURE FOR CONVERGING OT-IT

An IoT ecosystem consists of web-enabled smart devices that use software embedded systems, such as processors, sensors and communication hardware to collect, send and act on data they acquire from their environments. IoT devices share data from the sensor data by connecting to an IoT gateway or other edge devices where data is either sent to the cloud to analyse or analyse locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another device. These devices do most of the work without human intervention, although people can interact with them, to set them up, give them instructions and access the data [3].

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed. IoT can also make use of artificial intelligence (AI) and ML to aid easy and dynamic data collection processes. When a company decides to scale up its processes via IoT, it is not purely an IT discussion. IoT bridges the worlds of IT and OT such as control systems, data acquisition systems (DAQ) and industrial networks [16].

The architecture for converging IT-OT to enhance the security of business/industrial operations can be divided into three layers:

i. **IoT device layer**: This layer closes the gap that exists between the data world and physical world which starts with "things" or devices. The presence of accurate devices like sensors, actuators etc. that aid in generation of accurate data, as the bedrock of IoT, is very germane in providing products/services in the Industry 4.0 era. Examples of the leading IoT devices are Google Home Voice Controller, Amazon Echo Plus Voice Controller, Amazon Dash Button, August Doorbell Cam, August Smart Lock, Kuri Mobile Robot, Nest Smoke Alarm.
ii. **IoT gateway layer**: Due to the high level of data pre-processing, redundancy, interoperability, aggregation of data, connectivity, remote control and management, leads to the need for gateways [19]. A "gateway" refers to the physical device that functions as a link between sensors, cloud controllers, and intelligent agents for the purpose of providing additive security of the IoT network as well as the data packets transported by the network. That is, the layer controls all communication with sensors and remote connections. The IoT devices make use of a gateway as a central hub to deliver sensed knowledges and then communicate with the usser. Gateway stands between different IoT-enabled devices and the cloud (either public or private). IoT gateway ensures pre-processing of data at the edge in order to improve response times as well as provision of secure communication in both industrial IT and OT domains. Additionally, IoT gateway translates all types of mixed IoT connection into a single standard protocol.
iii. **IoT platform layer**: This layer interfaces with device and gateway layers and it connects the business, consumer applications and services as well as the management of the services. It interconnects with the first two layers. Without platform layer, it is impossible for IoT to function as software, including middleware popularly referred to *IoT cloud*. Simply put, IoT platform is a middleware lying between device gateway

layers. Thus, *data* on one hand and applications on the other hand. H*ence*, IoT platforms are known as *Application Enablement Platforms (AEPs)***.** An IoT platform enables IoT devices and endpoint management, connectivity and network management, data management, processing and analysis, application development, security, access control, monitoring, event processing and interfacing/integration. Some leading IoT platforms are Google Cloud Platform, IRI Voracity, Particle, Salesforce IoT Cloud, ThingWorx, IBM Watson IoT, Amazon AWS IoT Core, Microsoft Azure IoT Suite, Samsung Artik Cloud and Oracle IoT.

the SDG-9 achievable in the developoing countries.

Implications of the IoT Architecture on SDG-9

The IoT is no more a term any country, especially Nigeria as a developing nation, can ignore but instead a technology showing evidences of generating favourable socio-economic and environmental influences toward eradicating poverty. However, poverty eradication must go along with strategies that will build economic growth and as well as addressing series of social needs including health, health, social protection, education, and job opportunities without setting aside issues to tackle climate change and environmental

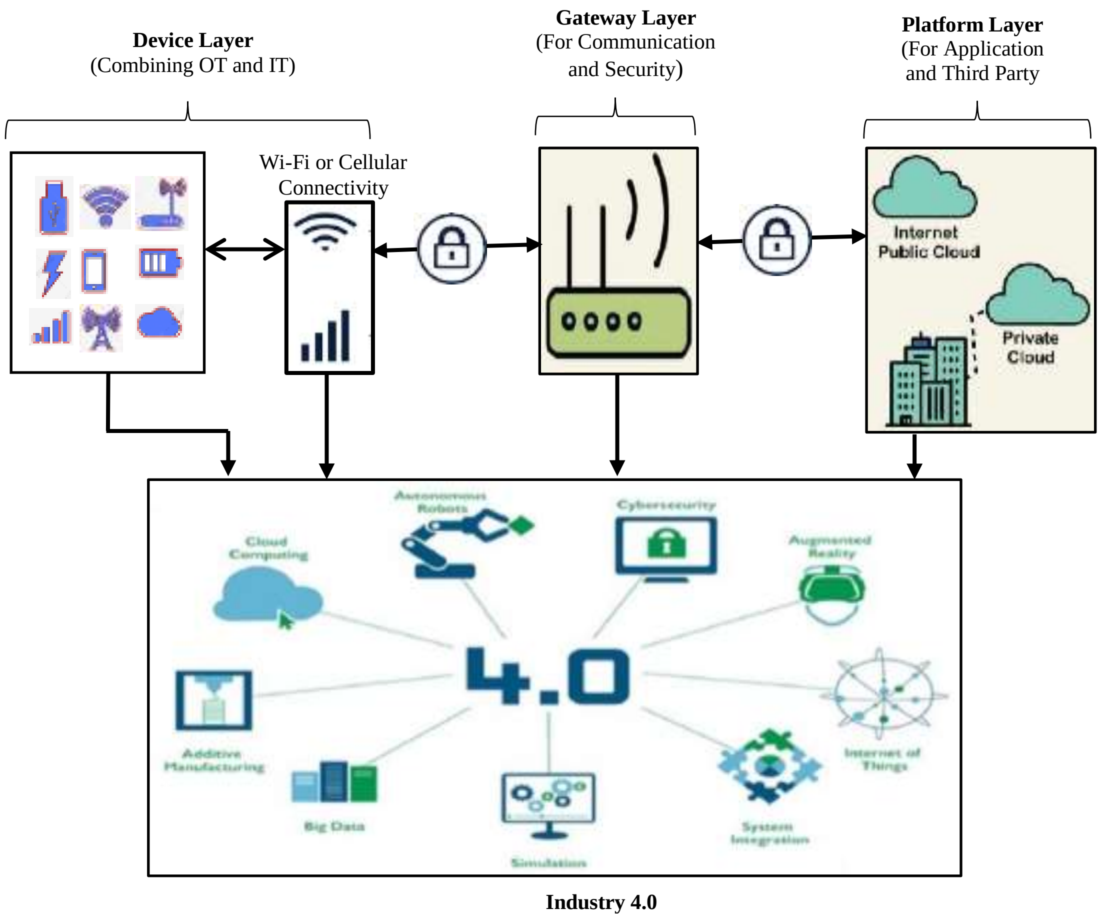

Figure 8: IoT Architecture Converging OT and IT for Industry 4.0

Figure 8 shows that different IoT devices that can be connected for communication via Wi-Fi or cellular method under secured environment using standard protocols in the gateway layer to provide services to the third party (i.e. end-user). These routines lead to the attainment of Industry 4.0 and thereby help to explore the objective of "Smart Indusrty" towards making

protection. As the SDGs call for action by all countries to enhance prosperity. According to Muraleedharan [22], IoT has presented 25% programmes addressing the SDG-9 with respect to all other aspects of SDG. This means that for developing countries to achieve the attainment of SDG-9, they must fully embrace and implement IoT architecture in the era of

Industry 4.0. Investing in IoT will no doubt make developing countires scale up with the developed countries in the areas of smart industy, city, transpartation, health etc.

5. Conclusion

Today, IoT technology imparts on the companies' competitiveness and betterment of citizens' quality of life for sustaninable development in the digital economy era of Industry 4.0. These factors are the germane reasons to commit huge resources towards further implementation of IoT technology by the developing countries including Nigeria. Other accruable benefits of IoT include reduction in the manufacturing cost, improved use of natural resources and preservation, enhanced product quality and regulatory compliance. However, security remains the issue of great concern by the developing countries as these so-called "borrowed" technologies come with security challenges without manpower and technical know-how to address them. As developing countries including Nigeria cannot perpetually remain indifference to modern technologies like IoT. Hence, in this paper, we have presented a robust security enhanced IoT architecture. The application of the architecture will allay the fear of developing countries toward the technology thereby making them beneficiaries SDG-9 in the digital economy era.

6. Recommendations

There is no doubt that every technolgical innvoation comes with its challenges. Aside security, the major challenging areas of IoT that hinder SDG-9 and digital economy bother on technical and commercial funding barriers. Consequently, it is recommended that concerted efforts be made by each developing country by formulating policies that will foster successful implementtation of IoT in the digital economy era powered by Industry 4.0. Also, Nigerian government should endeavour to provide enabling enviromnments and training of highly skilled security IT personnel through adequate funding for Industrry-4.0 to thrive and maximally reap the benefits inherent in digital economy as currently expereinced by the developed nations.

REFERENCES

[1] Al-Jayyousi, R.O. (2017). *Integral Innovation: New Worldviews*, London, United Kingdom published by Taylor & Francis Ltd.

[2] Sachs, D. (2014). Sustainable Development Goals for a New Era available online http://earth.columbia.edu/sitefiles/file/Sachs%20Writing/2014/HORIZONS_Sustainable%20Development%20Goals%20for%20a%20New%20Era_2014.pdf , 2014. [Accessed on 14/12/2019].

[3] Dubey, R., Luo, Z., Xu, M. & Wamba, S. F. (2015). Developing an integration framework for crowdsourcing and Internet of Things with applications for disaster response. In Proc. IEEE Int. Conf. Data Sci. Data Intensive Syst. (DSDIS), 520-524.

[4] Ganguli, S. (2015). The Impact of the IoT on Infrastructure Monitoring. Online: https://www.gartner.com/doc/3147818?srcId=1-2819006590&pcp=itg, 2015. [Accessed on 23/10/2020].

[5] Baro, E. A. (2011). Critical Examination of Information and Communication Technology Policies: Effects on Library Services in Nigeria. Available online: http://www.webpages.uidaho.edu/~mbolin/baro.htm [Accessed on 11/09/2020]

[6] Mutula, S. (2004). IT diffusion in sub-Saharan Africa: implications for developing and managing digital libraries. New Library World, 105(1202/1203), 281-289.

[7] Mwansa, B. (2017). The Role of Information and Communication Technology in Sustainable Development Goals in Africa: A Review. Texila International Journal of Academic Research, 4(2); 1-9.

[8] Rayes, A. & Salam, S. (2019). Internet of Things From Hype to Reality - The Road to Digitization Second Edition. Springer Nature Switzerland, pp. 393.

[9] Derhamy, H. (2018). Architectural Design Principles for Industrial Internet of Things. A PhD Thesis, Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, Lulela, Sweden.

[10] EDUCBA Introduction to Challenges of IoT Implementations, 2020.

https://www.educba.com/data-science/ [Accessed on 27/08/2020].
[11] Minerva, R., Biru, A. & Rotondi, D. (2015). Towards a de_nition of the internet of things (IoT), Tech. Rep.
[12] Ashton, K. (2009). That 'Internet of Things' Thing, In the real world, things matter more than ideas, 2009. Online: http://www.rfidjournal.com/articles/view?4986 [Accessed on 13/09/2020].
[13] Zaidan, A.A. & Zaidan, B.B. (2020). A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. *Artif Intell Rev* 53, 141–165. https://doi.org/10.1007/s10462-018-9648-9
[14] Dohr, A., Modre-Ospirian, R., Drobics, M., Hayn, D. & Schreier G. (2010). The Internet of Things for Ambient Assisted Living. Seventh International Conference on Information Technology: New Generations, ITNG, Las Vegas, Nevada, USA, 12-14.
[15] Ibrahim, M., & Huimin, M. (2017). Information Technology Components and Their Role in Knowledge Management for Product Design. *International Journal of Information and Education Technology,* 7(12): 948-953. doi: 10.18178/ijiet.2017.7.12.1001
[16] Bradicich, T. (2020). https://www.sas.com/en_nz/insight/articles/big-data/it-ot-convergence-the-dilemma-of-the-iot-perception-gap.html [Accessed on 30/04/2020].
[17] Cannaday, B. (2018). The IoT Analytics Lifecycle – From Generating Data to Predicting the Future. https://www.iottechexpo.com/2018/11/iot/the-iot-analytics-lifecycle-from-generating-data-to-predicting-the-future-losant/ [Accessed on 30/04/2020]
[18] Richter, F. (2015). Global Smartphone Traffic to Increase Tenfold by 2019. Online: http://www.statista.com/chart/3227/global-smartphone-traffic-to-increase-tenfold-by-2019/ [Accessed on 30/04/2020]
[19] *Windpassinger, N.* (2020). Internet of Things (IoT) active device connections installed base worldwide from 2015 to 2025. Online: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ [Accessed on 23/08/2020]
[20] DeStefano, T., K. de Backer & L. Moussiegt (2017). Determinants of digital technology use by companies, *OECD Science, Technology and Industry Policy Papers*, No. 40, OECD Publishing, Paris. http://dx.doi.org/10.1787/a9b53784-en
[21] Shea, S. & Haughn, M. (2017). IoT devices (Internet of Things Devices), https://internetofthingsagenda.techtarget.com/definition/IoT-device [Accessed on 23/10/2020].
[22] Muraleedharan, S. (2019). Role of Internet of Things (IoT) in Sustainable Development. https://www.ecomena.org/internet-of-things [Accessed 25/07/2020].
[23] Andreu A. (2020). Operational technology security - A data perspective. Journal of Network Security, 1: 8–13.
[24] Murray, G., Johnstone, M.N. & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. The Proceedings of 15th Australian Information Security Management Conference, 5-6 December. Edith Cowan University, Perth, Western Australia, pp.149-155.
[25] Jeff-Meyers, P.E. (2013). Best Practices for IT/OT Convergence. www.smartgridnews.com [Accessed on 9/02/2021].