International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

# Holistic Security for Internet-of-Things (IoTs) Implementation in Nigeria

**Engr. Fidelis C. Obodoeze**
Department of Computer Engineering Technology, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State, Nigeria

**Dr. Francis A. Okoye**
Department of Computer Science Enugu State University of Science and Technology (ESUT), Enugu, Enugu State, Nigeria

**Ifeyinwa Nkemdilim Obiokafor**
Department of Computer Science Technology, Anambra State Polytechnic, Mgbakwu, Anambra State, Nigeria

## ABSTRACT

The internet of things (IoT) is everywhere. It's in our homes, cars, offices and most commonly around our wrists. It's changing the way factories are run, how health care is delivered and how cities operate. With an estimated 5.5 million new "things" connected each day, and an expected 6.4 billion in circulation by the end of 2018, the IoT will increasingly become part of our lives. But with the IoT's proliferation comes great responsibility. You cannot take the security of the rapidly expanding IoT ecosystem for granted. Even the smallest, most minimally connected device must have the appropriate safeguards built in throughout its lifecycle. It is time to focus on IoT security at the point of design to securely manage devices from inception through implementation. The potential of IoT devices and sensors is enormous, even in Nigeria, but if the security of each device and application is taken lightly, it is very likely that the exploitation of unguarded vulnerabilities will stop the progress, preventing us from ever fully realizing that vast potential. This paper takes a comprehensive survey of the security architecture, vulnerabilities and challenges facing the successful implementation of IoT in Nigeria and proposed far-reaching and holistic security solutions to protect IoT devices/servers, the network and applications from being exploited by hackers, malwares and other undesirable elements so that the opportunities from IoT implementations will be realised in Nigeria in the nearest future.

***Keywords*** *: IoT ; vulnerability ; malwares ; DMZ ; holistic security ; Nigeria*

## 1.0 Introduction

THE Internet of Things (IoT) is opening up a world of real opportunities and rapidly transforming communities, cities and the daily lives of people worldwide. Today, the IoT encompasses more than 14 billion things connected to the Internet. The Internet of Things is connecting more and more devices. We're heading to a seamlessly connected world that will have 24 billion IoT devices by 2020. Connected devices are making headway into each and every aspect of our lives, including homes, offices, cars and even cities.

The IoT suggests a world where all humans and objects are connected via WiFi and other networks, constantly sending data back and forth. Objects may include machines, buildings, vehicles, sensors, actuators, mobile devices, computers, etc. Fig.1 illustrated health-care trends where IoT are used to monitor health status of patients. As reported by authors in [1], fig.2 depicts the possible devices that can be connected in IoT using common networks such as Local Area Network (LAN), Personal Area Network (PAN) and Wide Area Network (WAN).

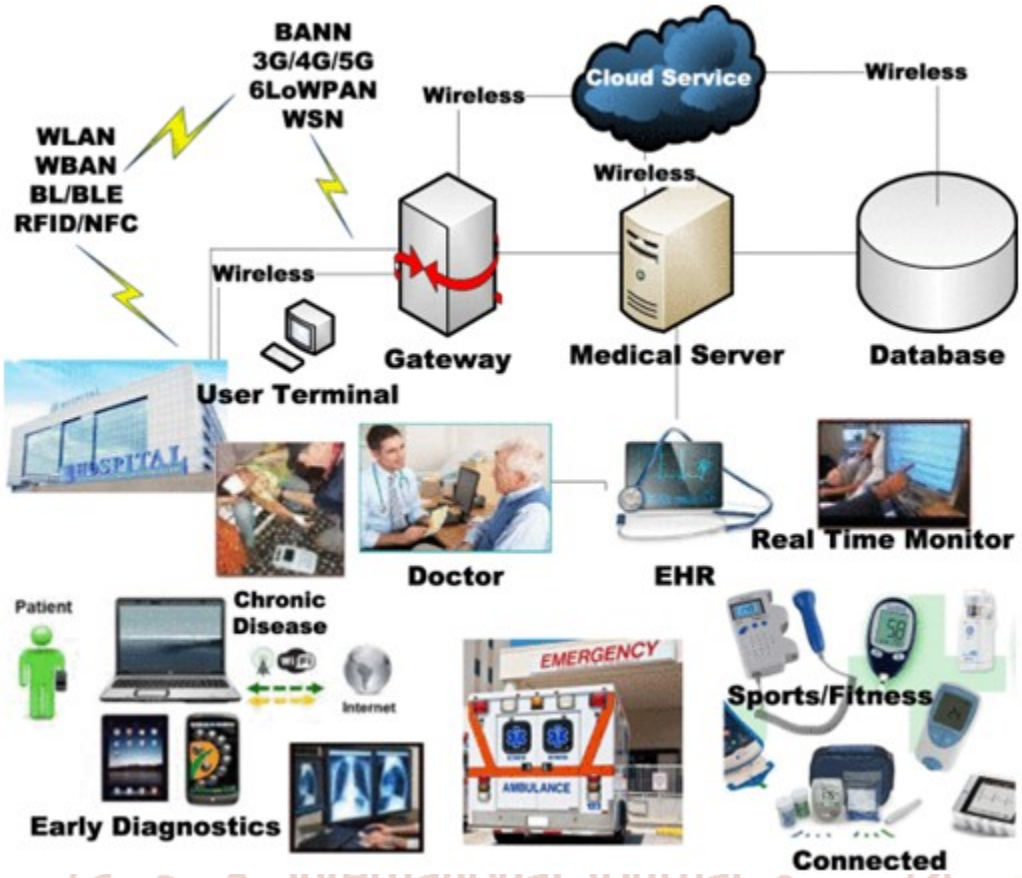


***Fig.1. Typical IoT connected devices with healthcare applications, Gateway and Servers [1]***

Already, reports have it that consulting companies are taking a close look at IoT and are predicting a rosy future for the technology with forecasts of compound yealy growth rates (CAGR) of between 30 and 33 per cent over the next four years .

The IoT is seen to have the potential to be much larger than the existing Internet. According to Cisco's Internet Business Solutions Group, it recently predicted that some 25 billion 'things' will be connected to the Internet by 2015, and 50 billion by 2020.

Already, the globe has been projected to realise about $19 trillion through the application of IoE, about $500 billion is expected to be available to Nigeria, South Africa, Kenya and other sub-Saharan African countries in another 10 years [2]. This increased connectivity now assures we are able to do things like never before. However, with this connectivity there comes a flipside. Some of these devices will originate from locations which are not secured. IoT is becoming an attractive and easy target for cybercriminals. The challenge is security- how do we secure billions of devices, objects, servers, humans from hackers and malwares' exploitation and abuses.

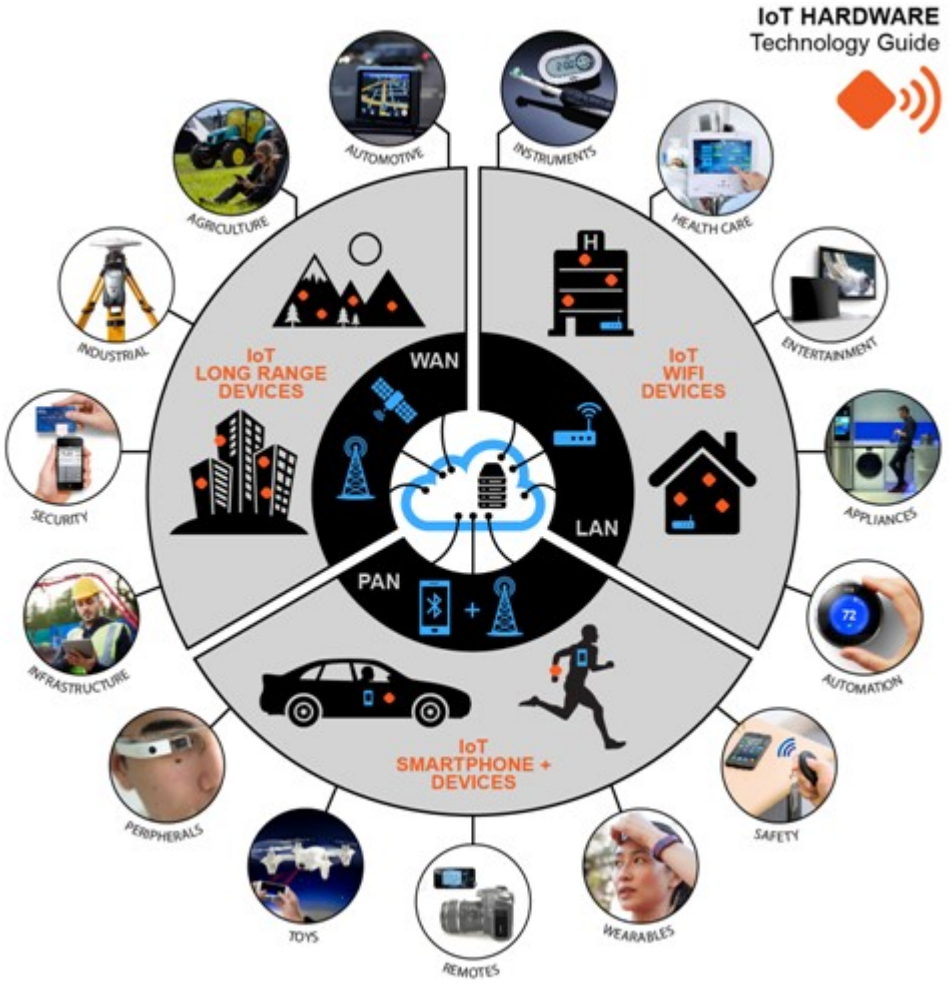


***Fig.2. Typical IoT connected devices using LAN,PAN and WAN***

In contrast to human-controlled devices, IoT devices are always connected and functioning. IoT devices go through one-time authentication which makes them vulnerable to infiltration and nefarious attacks. Each type of IoT device might be vulnerable to different kinds of attacks, most not yet invented. The devices themselves have different levels of security, and some might have no security at all. As with anything, the convenience factor offered by IoT devices can also come with a sacrifice in security. Often times, engineers or developers of IoT devices are not trained in security or secure coding. Additionally, manufacturers of many of these devices do not have systems in place to deploy software updates or patching paths. Once they have realized the revenue from the sale of a device, there is no incentive for them to continue to monitor and fix security issues identified within their devices. Given the lack of technical expertise of most end users, updates and proper location identification of IoT devices is a major concern.

End users typically just want to plug a device in and go — without understanding the implications of how and where they install the device. Although, some of these devices do have auto-updates, most do not. If a device is left unpatched for a long period of time, a greater percentage of vulnerabilities will be identified. Placing an unsecured IoT device on the same subnetwork as an end-user's home PC and mobile devices can allow an attacker to easily pivot to attacking these more valuable assets.

Another reason hackers may want to target IoT devices is because if they find a vulnerability in one device, it will very likely apply to many other devices. Some IoT devices are just like small Linux computers. For example, a hacker could use them to conduct DoS attacks.

Therefore, strong security mechanism needs to be implemented on these gateways as well as the devices and applications to improve the overall security of the system.

### 1.1 IoT security Architecture Tiers

There are three (3) major tiers in IoT architecture. They include :-

1. **Devices/Gateways tier**: Protect against a "fake" server that sends malicious commands, or protect against a hacker that tries to listen to private sensor data being sent from the devices.
2. **Network/Transport tier**: Protect against a "fake" device that sends false measurements that might corrupt the data that is being persisted in the application.
3. **Applications tier:** Protect against the invalid use of data, or protect against the manipulation of analytical processes that are running in the application tier.

The application layer of an IoT device provides the largest attack surface to hackers [3]. The application layer includes any application that has connectivity with the IoT device, which can include local web applications, cloud-based applications, and mobile apps.

Application security must be an intrinsic part of the software development lifecycle (SDLC) for all IoT applications, particularly during the design, development, and testing stages. Within the planning or design stage of an IoT application, there must be a formal "top-to-bottom" assessment of the planned application's security and privacy requirements.

### 1.2 IoT security basics

IoT solutions involve a complex network of smart devices, such as vehicles, machines, buildings, or home appliances, that are embedded with electronics, software, sensors, and network connectivity, which enable these "things" to collect and exchange data. The "things" in the Internet of Things allow developers to provide a broad range of new services based on these cloud-enabled, connected physical devices. As IoT applications collect more and more previously unexposed—often private—data, and allow access to various control functions over the internet, security becomes a major challenge. Therefore, an IoT application must achieve the following objectives:

1. *Prevent system breaches or compromises*
2. *Support continuous monitoring*
3. *Be resilient or strong*

***1. Prevent system breaches or compromises.***

Each tier of the IoT application must implement effective preventive measures to keep the hackers out. For example, you need to harden the device to make sure communication from the device to the cloud is secure.

2. ***Support continuous monitoring.***

Even the best secured systems still leave much vulnerability. Also, today's best secured solution (both hardware and software) might not be good enough to prevent attacks in the future. Therefore, you must supplement your security measures with continuous monitoring and constant upgrading of the system to protect against the latest forms of attack.

***3. Be resilient.***

Finally, if a breach does occur, damage must be minimized and the system must recover as quickly as possible.

### 1.3 IoT vulnerabilities

Developers have so many ways that they can apply IoT technologies to create IoT solutions. They can create a simple home monitoring system that provides alerts to smartphones and smart watches, or they can create complex healthcare systems that collect data and control a network of patient devices—and many opportunities for solutions we can't yet imagine [3].
But connecting objects like cars, homes, and machines exposes a lot of sensitive data, such as the location of people in a building or medical records of patients. This data must be protected in accordance with the key information security principles, the CIA triad: confidentiality, integrity, and availability [3].

Any device that has network connectivity is vulnerable. Personal data that is collected by IoT devices is always of value to data hackers and identity thieves. Also, a cyber attack on IoT solutions has the potential to cripple physical services and infrastructure. For example, hackers attacked a Jeep Cherokee while it was being driven on a highway. Therefore, secure IoT applications are not only critical for the reputation of the enterprise, but also for the physical health and well-being of the clients and users of the solution [3].

### 1.4 IoT security design challenges

While the importance of IoT security is widely understood and agreed upon, the actual design and

implementation of IoT security brings new challenges and opportunities for creativity. In the design of most any app, developers always face a trade-off between security and usability. For IoT solutions, it becomes even more problematic. IoT devices often have limited computing power and memory capacity, making it difficult to use complex cryptographic algorithms that require more resources than the devices provide.

Another challenge is updating IoT devices with regular security fixes and updates. Rolling out security patches to all devices at once can be very difficult in unreliable, low-bandwidth device networks, and many existing security measures, such as web browser security, might not be available to IoT applications.

In addition, security mechanisms might need to be developed or enhanced for new protocols that are designed specifically for the Internet of Things, such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP). Therefore, it is especially important to factor in security considerations from the very beginning when you design IoT apps.

## 2.0 Our Proposed Security Framework for IoT Implementation in Nigeria

The researchers proposed an IoT implementation roadmap for Nigeria in 2016 in [4] as depicted in Fig.3. Here, the proposed operational security framework for the interconnection and control of smart objects/things participating in IoT in Nigeria.

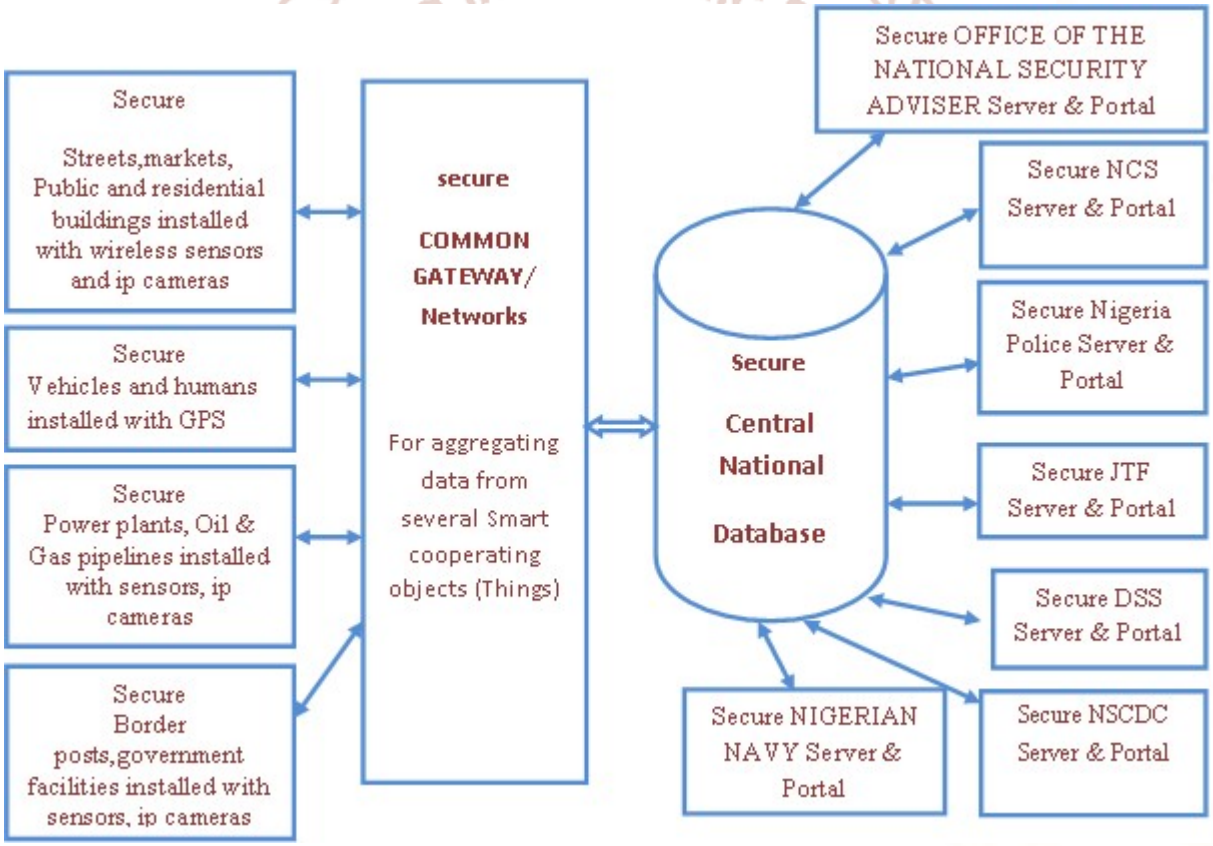


***Fig.3. The proposed IoT Implementation framework in Nigeria***

The proposed implementation framework in Fig. 3 is meant to aggregate security data from various collection points – streets, markets, public and residential buildings, oil and gas pipelines, border postings, power plants/equipments, private and public vehicles, human beings etc. installed or embedded with *smart objects* or *things* to monitor and route data to the national Common Gateway. These data are then sent to the Central National Database which can be accessed by the various security agencies (through their corprate intranet/internet portal) such as Nigerian Customs Service (NCS), The Nigerian Police Force, The Nigerian Security and Civil Defence Corps (NSCDC), Directorate of State Security (DSS), Joint Military Task Force (JTF), The Nigerian Navy, The Office of National Security Adviser. The Central National Database is secured as well as the various

portals of the security agencies so that unauthorised access is not allowed.

The Common Gateway module of the proposed National Security Framework in Fig.4 is a fusion of many gateways for RFID tracking objects, GPS tracking objects, WSN tracking objects, surveillance security cameras. A software methodology is used to combine them effectively into a common gateway so that they can come together and their output data channeled into a common central database and then to a common internet/intranet portal so that law enforcement and security agencies can access the portal real-time and get updated information about any security lapse, threat or attack anywhere in the country.

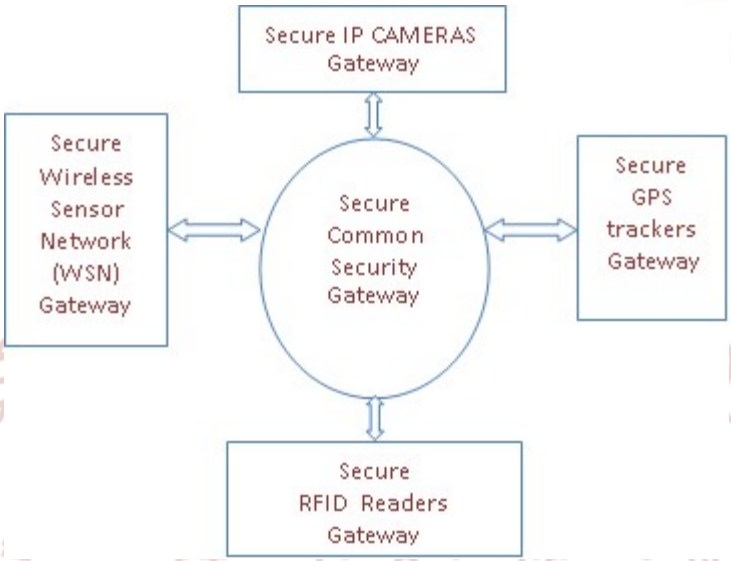


***Fig. 4 The integration of different gateways from WSN, RFID, GPS and surveillance security cameras into a common gateway***

### 2.1 Security Requirements to protect the proposed IoT framework from Hackers

For any system to be considered secure, it must meet three (3) basic security requirements of CIA- Confidentiality, Integrity and Availability.

The proposed IoT framework must involve three (3) stakeholders: 1. The devices/servers 2. The network 3. The application/solutions

From any of these three stakeholders, an attack can come from cybercriminals or hackers or even malwares to steal data, modify data or disrupt the network from rendering services. Any security solution to protect IoT implementation must include the three (3) security requirements and must cover the three stakeholders, otherwise there will be vulnerability for hackers to exploit and cause havocs.

From Fig.3, it can be deduced that attacks or security vulnerability can come from three standpoints as described in the following section.

#### 2.1.1 The application/solutions

The applications here include:-

*1. The National Database*
*2. The Portals/servers*

**Security for the Applications:**

This layer includes applications, portals, websites, apps, central database. This layer is the most prone to attack by hackers and malicious program such as malwares. The software developers must include inbuilt designs that must prevent this type of attack. Other security measures to protect the Applications include:

1. ***authentication,***
2. ***authorization,***
3. ***access control list,***
4. ***selective disclosure,***
5. ***intrusion detection,***
6. ***firewall, and***
7. ***Antivirus program installation and constant updates.***

Authentication and authorization protect the application from being accessed by criminal-minded individuals such as hackers and malicious software such as virus, spyware, worms and botnets. Authentication and authorization are implemented using passwords, pin codes, encryptions, hash keys etc. Access control list presents the application with the list of authorized people who are permitted to login into the IoT application. This list has different authorization levels for each user. Selective disclosure entails the application having data that have different levels of usage; some users can have access to some data while some will have access to some other data. Intrusion detection is inbuilt mechanisms in devices, gateways and applications that assist them to track any attack or security breach and raise necessary alarm. Anti-virus program is good candidate towards detecting malwares and neutralizing them. Anti-virus software is also a good candidate for intrusion detection because it contains all the needed components to detect hackers' attacks as well as malwares'.

Fig. 5 depicts how applications and its gateways can be protected using firewall and Demilitarized Zones (DMZs) to wade off malwares and hackers.

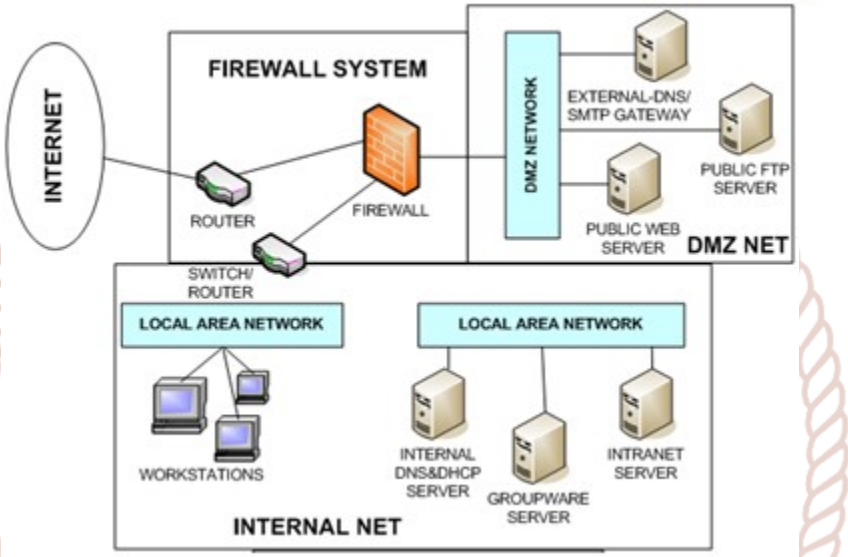


***Fig.5. Multi-homed Host Firewall with Demilitarized Zone (DMZ)***

### 2.1.2 The Network/Gateway

The Network may include:-

1. **The Common Gateway** that aggregates data from several things or smart objects such as sensors, devices, machines, buildings, markets, street lights, borders, humans, vehicles , etc.
2. **The connecting Network** such as GSM Telecomm or cellular networks or 2G/3G communication network e.g. MTN, Glo, Airtel, 9Mobile, WiFi, WiMax, Bluetooth, GPRS, fibre optic cables, fixed telephone networks and closed IP data networks etc.

**Security for the Network:**

The security of network layer can be examined in two main sub-layers; *wireless* and *wired*. One of the initial actions in wireless security sub-layer is the development of protocols for authentication and key management [5]. For example; SSL/TLS is developed to encrypt the link in the transport layer, and IP security protocol (IPSec) is developed to keep the network layer secure. They can provide authenticity, confidentiality and integrity in the each layer [6]. Also, using PPSK (Private Pre-Shared Key) for each sensor or device connected to the network provides another security measure for IoT system. By providing different unique keys, the access domain for each type of device can be defined easily. Moreover, disabling guest and default passwords in network devices such as routers and gateways should be done immediately upon installing a new network device. This includes strong password policies, password management and periodic change of passwords [7]. The wired security sub-layer is concerned with devices, which communicate with other devices on the IoT system using wired channels. Common security techniques are applied in wired type networks are firewalls and Intrusion Prevention System (IPS). If the network has firewall or IPS, it can inspect network

packets deeply that are destined towards the destination. However, existing IoT has no ability in terms of packet inspection and packet filtering. There is an ongoing research on this issue where security researchers try to design a low resource-hungry firewall for IoT to provide the ability of packet inspection [8].

### 2.1.3 The Devices

The devices may include mobile devices, wrist watches, sensors, actuators, RFIDs, GPS trackers, ip camera, machine, computers (including servers), buildings, etc. that are connected to exchange data with one another and with the common gateway.

**Security for the Devices:**

Security devices or equipments such as RFID readers, sensors, actuators, GPS tracking devices and other devices require to be secured efficiently. Device manufacturers must do the needful to protect the devices during the design stage of the devices. The users must also imbibe security consciousness and precautions to safeguard themselves and their devices during communication. Some of the common problems we have seen with IoT devices are:

- ***Hardcoded passwords***
- ***Code injection***
- ***Unsecure API***
- ***Web application vulnerabilities***
- ***Lack of encryption in communication***

1. ***There must be physical security for these devices***. The first step is to ensure that only authorized people can have access to sensitive data produced by physical objects, that's why a physical identity and access management policy need to be defined.
2. ***There must be Authentication and authorization*** requirements from IoT. This will help only authorized and genuine devices to connect to the network and communicate with one another.
3. ***Risk Assessment*** is a fundamental of IoT security which determines the extent of the potential threat and the risk associated with an IoT system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.
4. ***There must be encryption of data during communication sessions*** between one device or the other or one 'thing' to 'another thing'. Cryptographic processing is one of the main tasks in security mechanisms for sensor data on IoT. These operations that are often used in order to guarantee privacy of data include encryption and decryption, key and hash generation, and sign and verify hashes.
5. ***There must be security in multimedia data collection*** to protect multimedia data such as image, graphics, and audio. Security techniques such as multimedia compression, stenography, water marking, encryption, time session and intellectual property can be applied here.

## 3.0 Summary and Conclusion

IoT usage and adoption is rising in Nigeria and elsewhere. Billions of devices are now connected to the network so that machines, humans, building, and devices can interact from anywhere with each other. Its prospects in increasily in Nigeria and other parts of the world but the greatest challenge to the realization of its potentials is security vulnerability and threats.

These security threats affect these triads- the devices, the networks and the applications. A holisitc security solution framework must therefore provide or suggest security solutions that will cover these triads in mind. Until these three security solutions are provided for the triads, IoT implementation benefits will continue to elude Nigeria and other developing countries.

This paper presented an implementation security framework for IoT for Nigeria and suggested various security mechanisms this framework can be implemented to guarantee a holistic secuirity for the devices, the network and the applications.

## References

1. S. M. Riazul Islam, Daehan Kwak , MD. Humaun Kabir, Mahmud Hossain, Kyung-Sup Kwak, 'The Internet of Things for Health Care: A Comprehensive Survey', IEEE Xplore, Vol.3, 01 June 2015. Accessed online at http://ieeexplore.ieee.org/document/7113786/.
2. Adeyemi Adepetun, 'Preparing Nigeria for Internet of Things', The Guardian Newspaper, 25th Novemner, 2015. Accessed online at https://guardian.ng/technology/preparing-nigeria-for-internet-of-things/

3. Amitranjan Gantait, Joy Patra, and Ayan Mukherjee, 'Design and build secure IoT solutions, Part 1, Securing IoT devices and gateways', IBM DeveloperWorks, May 16, 2016. Accesed online at https://www.ibm.com/developerworks/library/iot-trs-secure-iot-solutions1/index.html

4. Fidelis C. Obodoeze, Chris O. Onyibe, 'internet-of-things (iots) and smart objects – the solution to nigeria's security challenge', Proceedings from the First National Conference, School of Engineering Technology, Akanu Ibiam Federal Polytechnic Unwana, June 21-25th 2016, pp.11.

5. Jara, A.J., Ladid, L. and Skarmeta, A. (2013) The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4, 97-118.

6. Suo, H., Wan, J., Zou, C. and Liu, J. (2012) Security in the Internet of Things: A Review. IEEE International Conference on Computer Science and Electronics Engineering, Hangzhou, 23-25 March 2012, 648-651. https://doi.org/10.1109/ICCSEE.2012.373

7. Zolanvari, M. and Jain, R. (2015) IoT Security: A Survey. http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec/index.html

8. Gupta, J., Nayyar, A. and Gupta, P. (2015) Security and Privacy Issues in Internet of Things (IoT). International Journal of Research in Computer Science, 2, 18-22.