World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.218

DEVELOPMENT OF AN INTERNET OF THINGS PIPELINE MONITORING SYSTEM

K. C. Anyanwu*, G. A. Chukwudebe and R. E. Ogu

Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria.

Article Received on 18/03/2018 **Article Revised on 08/04/2018** **Article Accepted on 29/04/2018**

***Corresponding Author**
K. C. Anyanwu
Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria.

ABSTRACT

This paper presents an Internet of Things Pipeline Monitoring System (IoTPMS) for onshore crude oil pipelines. The IoTPMS prototype developed in this research comprises of an Arduino Mega 2560 microcontroller, an Arduino Wi-Fi shield 101, a HC-SR501 PIR motion detection sensor, a YF-S201 flow rate sensor, a power supply unit and the ThingSpeak platform. A waterfall software model was used to develop the design requirements and specifications of the IoTPMS prototype and also to program the assembled and interconnected hardware components of the system. With the implementation of this model, once the IoTPMS prototype is put in operating condition using the demonstration apparatus and powered ON, it scans for available Wi-Fi networks and connects to a configured Wi-Fi network. As long as it stays connected to the Wi-Fi network, it will be getting intrusion and flow rate data from the sensors and uploading these data to the Pipeline Monitoring System channel on the ThingSpeak platform. The result of this work is a fully functional IoTPMS prototype that can monitor the flow rate of the fluid flowing through onshore crude oil pipelines, third-party intrusion along the right of way of onshore crude oil pipelines and transmits these data and location through the Internet to a secure ThingSpeak IoTPMS channel every 20 seconds for data analysis and real-time remote monitoring of onshore crude oil pipelines to ensure their safety.

KEYWORDS: Internet-of-Things, Pipeline-Monitoring, Flow-Rate, Intrusion-Detection, Thing Speak, Data-Analysis.

INTRODUCTION

Nigeria is Africa's top exporter of crude oil with an average of over 2 million barrels exported per day (OPEC, 2016). Nigeria's Oil and Gas industry accounts for about 35 percent of Nigeria's Gross Domestic Product (GDP) and petroleum exports revenue represents over 90 percent of Nigeria's total exports revenue (OPEC, 2017). This means the Nigerian Oil and Gas industry is the main contributor to Nigeria's economy and crude oil export the major export commodity. Large proportions of Nigeria's crude oil are produced onshore and are transported through extensive systems of pipeline networks that run from the oil wells to the export terminals and refineries which makes these pipeline networks the heartbeat of the Nigerian Oil and Gas industry.

Pipeline construction materials just like every other engineering material is subject to aging, corrosion, wear, tear, extreme weather conditions and other environmental factors that can result in the natural breakdown of pipelines leading to crude oil spillage without a third-party vandalizing the pipelines. Secondly, the activities of vandals such as crude oil thieves and militants pose the biggest threat to the security of crude oil pipelines with the latter resulting in the drop of Nigeria's crude oil export rate from 2 million barrels a day to 1.5 million barrels a day (Kachikwu, 2016).

The above stated problems have negative socio-economic impacts which include water pollution, soil pollution, the degradation and destruction of the ecosystem, health hazards and loss of revenue. This research seeks to explore the capabilities of the Internet of Things (IoT) technology to develop a prototype Internet of Things Pipeline Monitoring System (IoTPMS) for onshore crude oil pipelines. The IoTPMS prototype developed in this research is a unit of the distributed sensing system that can monitor onshore crude oil pipelines, obtain real-time data of the condition of pipelines and transmit captured data through the Internet to a data analytics platform for real-time remote monitoring of these pipelines from anywhere on the globe in a bid to complement the efforts of the security operatives on ground that work round the clock to secure onshore crude pipeline installations in Nigeria.

LITERATURE REVIEW

Some of the related literature reviewed in the course of this study with the aim of filling research gaps and coming up with a pipeline monitoring system that can adequately ensure the security of onshore crude oil pipeline networks are highlighted as follows:

Shoewu, *et al*., (2013) proposed a microcontroller based alarm system for detection of pipeline vandals. The system makes use of a pressure sensor, a light sensor and Passive Infrared (PIR) motion detection sensor to detect break or vandalism of pipeline. The drawback of this system is that it cannot allow real-time remote monitoring of pipelines. It is also subject to fluctuations in GSM network in different terrains and it also has no functionality for web-based interface to monitor the pipelines which is an essential requirement for IoT. It also has an alarm which will make vandals aware of a security system in the vicinity. The exposure of the system will make it an easy target for vandals.

Ezeh, *et al*., (2014) proposed a pipeline vandalisation detection alert system with SMS. The system presented here is a remote pipeline monitoring system with location specifications. It makes use of a continuous electrical path which is provided by a resistant sensor and a break in the signal path will cause cessation of the signal and provide detectable change in the state of the system. This results to triggering of an alarm and notification by text message (SMS) to an operator's mobile phone. The research gap here is that it is GSM based and therefore has no capability for Internet based monitoring which is an essential requirement for IoT implementation. It also has an alarm which will make vandals aware of a security system in the vicinity. The exposure of the system will make it an easy target for vandals.

Obodoeze, *et al.,* (2014) provided insights on the way an automated electronic surveillance and monitoring system can be used to detect, alert and dispatch video/photo footage of an oil pipeline vandalization incident from a remote location to oil pipeline operators at the control station. They proposed a method for providing automated detection for pipeline with remote monitoring and location specification using a PIR sensor to detect early intrusion of vandals into the pipeline system in order to communicate to the pipeline operators via SMS and email alerts. The drawback of this system is that the system is bulky and also exposed because of the overhead camera which will make it an easy target for vandals and oil thieves.

Ononiwu, *et al*., (2014) proposed a real-time oil pipeline anti-intrusion system using acoustic sensors. This proposed system involves the transmission of audio tones using acoustic and Dual Tone Multi-Frequency (DTMF) signaling through wires laid along the pipeline network. The research gap here is the delay in the transmission of signals to the control station from longer distances along the pipeline network.

Igbajar and Barikpoa (2015) in their work proposed an intelligent microcontroller based pipeline monitoring system with alarm and sensor. Their research is on developing an intelligent architectural design and model for real-time detection of oil spillage using an automated crack and vandalism detection alarm and SMS alert for pipelines with remote monitoring and location specification. The system was designed in such a way that whenever a leakage is detected in the pipeline, it will trigger alarm and send an SMS to the control unit. The research gap in this design is that is it GSM Based and therefore cannot enable web-based or online-based remote monitoring which is an essential requirement for IoT implementation. It also has an alarm which will make vandals aware of a security system in the vicinity which makes it an easy target for vandals.

MATERIALS AND METHOD

The hardware materials used in the course of this research are Arduino Mega 2560 Board, HC-SR501 Passive Infrared (PIR) Motion Sensor, YF-S201 Hall Effect Water Flow Sensor, Arduino Wi-Fi Shield 101, connecting wires, Laptop, Type A to Type B USB Cable, PVC enclosure, PVC pipes, DC Adapter, Plastic containers, plastic water tap and Teflon tape. The software tool used in designing the circuit is PCB Artist, the software codes are written in C Language, while the software tool used in compiling and uploading the codes of the circuit is Arduino Integrated Development Environment (IDE).

A. Design Requirements of the IoTPMS

in order to remotely monitor onshore crude oil pipelines in real time, the IoTPMS prototype should be able to monitor the rate of flow of fluid flowing through the pipe and detect any change in pressure, the system should be able to detect intrusion along a given distance of the pipe and finally, the system should be able to connect to the Internet and transmit the acquired data to an end user which can be accessed using an array of electronic and smart devices such as computers, tablets, phones etc for data analysis and determination of the actual cause of drop in pressure of the fluid flowing through the pipe which could be as a result of vandalism or natural breakdown of the pipe.

The system would require a power supply, sensors for data acquisition, a controller and a means of sending the acquired data to an end user using the Internet. The block diagram of the modules for the realization of the stated requirements is shown in Fig. 1.

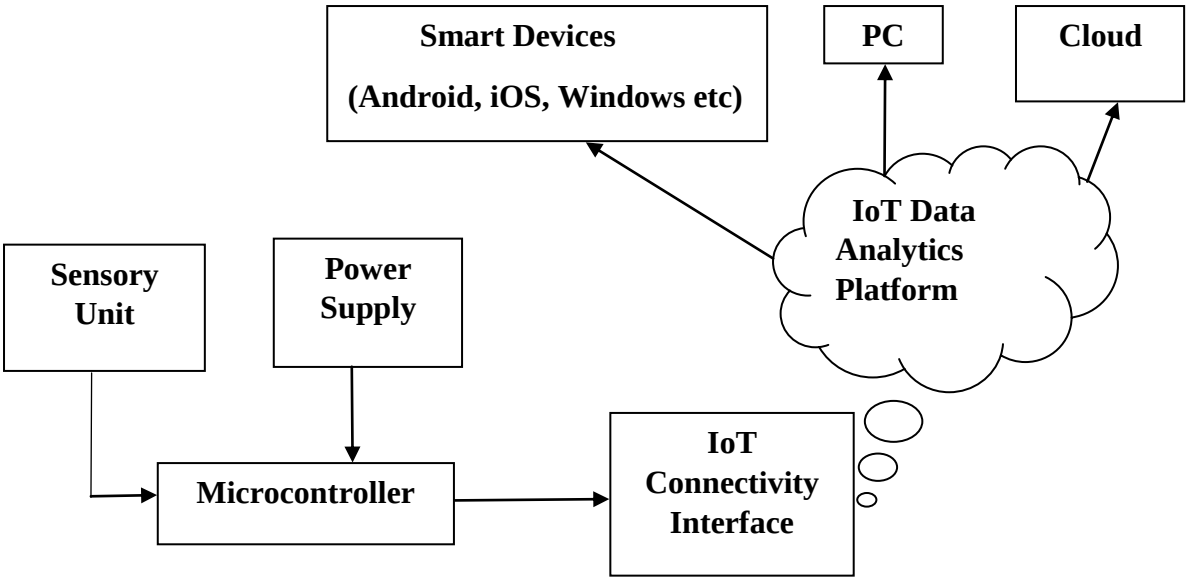

Fig. 1: Block Diagram of the Internet of Things Pipeline Monitoring System.

1) Power Supply Unit

The power supply unit provides the current and voltage requirements of the various blocks that make up the system. The power supply of the IoTPMS prototype is obtained from a 9V DC adapter to the microcontroller, although it can still be powered through the Universal Serial Bus (USB) port of the microcontroller. The microcontroller in turn powers all the other hardware components of the IoTPMS prototype as they are all connected to it.

2) The Sensory Unit

The sensory unit is responsible for the data acquisition of the system. The sensory unit of the IoTPMS prototype is made up of the flow rate sensor and the motion detection sensor. The YF-S201 Hall Effect water flow sensor was used in this prototype for measuring the rate of flow of fluid through the pipe. It is responsible for producing the signals that the microcontroller responds to for detecting flow rate and it has a maximum output of 30 litres per minute. The HC-SR501 PIR motion detection sensor is responsible for producing the signals that the microcontroller responds to for detecting intrusion and it has a sensing range of 6 meters.

3) The Microcontroller

The microcontroller used in this research is the Arduino Mega 2560. It is a microcontroller board based on the ATmega1280. It is powered by a 9V DC adapter, although it can still be powered through its Universal Serial Bus (USB) port. The function of the microcontroller is to coordinate the input and output requirements of the IoTPMS prototype.

4) The IoT Connectivity Interface

The IoT connectivity interface is the unit that is responsible for connecting the IoTPMS prototype to the IoT data analytics platform through the Internet. The connectivity method used in this research is wireless connectivity. The Arduino Wi-Fi Shield 101 board was used as the Internet connectivity interface in this research. It is a self-contained system on chip (SoC) that can give any microcontroller access to a Wi-Fi network. It is capable of either hosting an application or offloading data over a Wi-Fi network.

5) IoT Data Analytics Platform

The IoT data analytics platform is an Internet platform that is configured for IoT application, data gathering, analysis and manipulation. The ThingSpeak platform was chosen as the IoT data analytics platform for this research because it a free IoT platform for data collection, analysis and manipulation. The ThingSpeak platform is also user friendly and has features like Google map location.

Fig. 2 is a snapshot of the ThingSpeak Pipeline Monitoring System Channel on a web browser after its creation. The channel displays information such as the Channel name, Channel I.D, the Channel access type and the purpose of the Channel. The real-time status of the IoTPMS prototype can be viewed by logging onto https://thingspeak.com/channels/398173 and using the log in credentials to sign in.

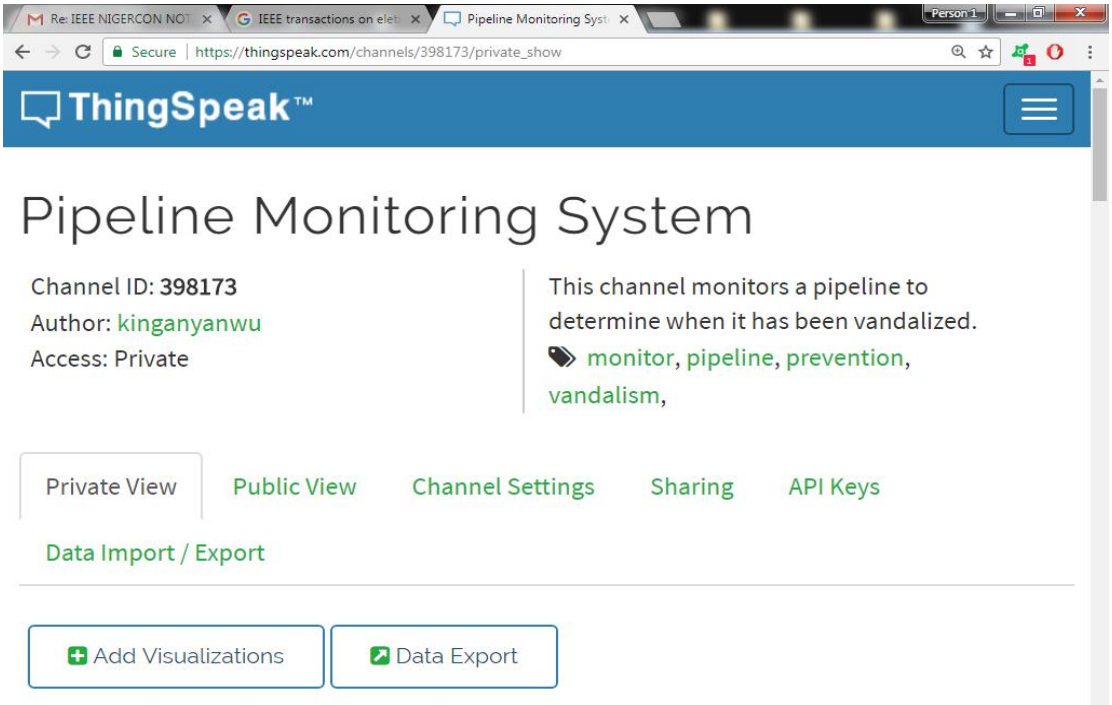

Fig. 2: ThingSpeak webpage showing the IoTPMS Channel.

B. Prototype IoTPMS Implementation

The Arduino Wi-Fi Shield 101 was mounted on the Arduino Mega 2560 board. The outputs of the PIR motion detection sensor and the water flow sensor are connected to ports A_0 and PWM_2 of the Arduino Mega 2560 respectively through the Arduino Wi-Fi Shield 101. The input voltage of the sensors is supplied through the 5V port of the Arduino Mega 2560 and the sensors are grounded using the ground ports on either side of the Arduino Mega 2560. The water flow sensor is installed in the line of flow of the pipeline while the PIR motion detection sensor is deployed in the open to detect intrusion. All the connections were made with wires and after the connections were made, the software codes were uploaded to the Arduino Mega 2560 through its USB port.

Fig. 3 is the flowchart of the algorithm of the IoTPMS showing the various steps involved in the operation of the IoTPMS prototype.

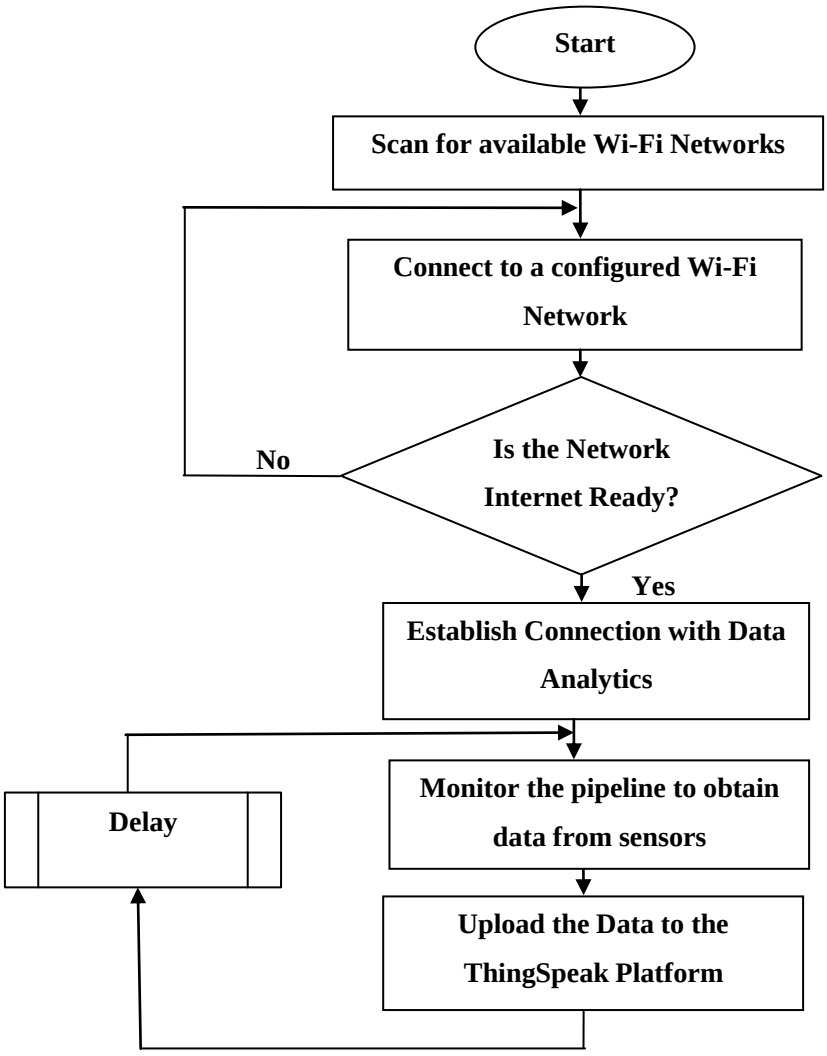

Fig. 3: Flowchart of the Algorithm of the IoTPMS Prototype.

When IoTPMS prototype is turned is put in operating condition and turned ON, it scans for available Wi-Fi networks and connects to an already configured Wi-Fi network. If the Wi-Fi network is Internet ready, the IoTPMS prototype establishes connection with its data analytics channel on the ThingSpeak platform. If the Wi-Fi network is not Internet ready, the system repeats the cycle of connecting to the configured Wi-Fi network and this cycle will continue until the configured Wi-Fi network is Internet ready.

After Internet connectivity has been established with the ThingSpeak platform, the system continuously obtains flow rate and intrusion data from the sensors and uploads these data to the Pipeline Monitoring System channel on the ThingSpeak platform every 20 seconds. Fig. 4 is a picture of the completed IoTPMS prototype.

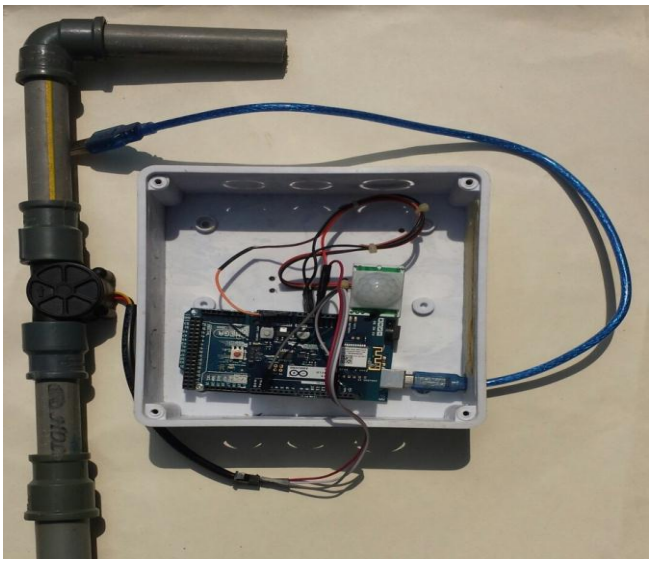

Fig. 4: Complete IoTPMS Prototype.

RESULTS AND DISCUSSION

The demonstration apparatus used in testing the IoTPMS prototype include a plastic gallon which serves as a water reservoir, two buckets for water supply, PVC pipe that fits into the reservoir and has a tap for varying the pressure of the water flowing through the pipe. The flow sensor is installed along the pipe in the direction of flow of the water flowing through the pipe and it detects any variation in the pressure of water flowing through it, while the PIR motion detection sensor was deployed in the open for intrusion detection.

Intrusion was tested by human movement within the sensing range of the PIR motion detection sensor while variation in flow rate of water was achieved by varying the rate of flow of water through the water flow sensor using the tap. The IoTPMS prototype developed

in this research was tested with water instead of crude oil because of the flow rate sensor deployed in the design of the prototype. Using crude oil to test the YF-S201 Hall Effect water flow sensor would have yielded differences in the accuracy of the results gotten because the sensor is already calibrated to function with water and the density and viscosity of water and crude oil vary.

The sensors capture different independent data and upload them to the ThingSpeak Pipeline Monitoring System channel in two different fields which are the Flow Rate (Field 1) Chart and the Intrusion Detector (Field 2) Chart. The red dots on the field charts represent the data updates sent to the ThingSpeak platform by the IoTPMS prototype every 20 seconds for data comparison and analysis.

Fig. 5 and 6 are snapshots showing the flow rate and intrusion detection field updates of the IoTPMS prototype to the ThingSpeak IoTPMS Channel on a web browser. It also displays the time of the updates and the date of the updates.

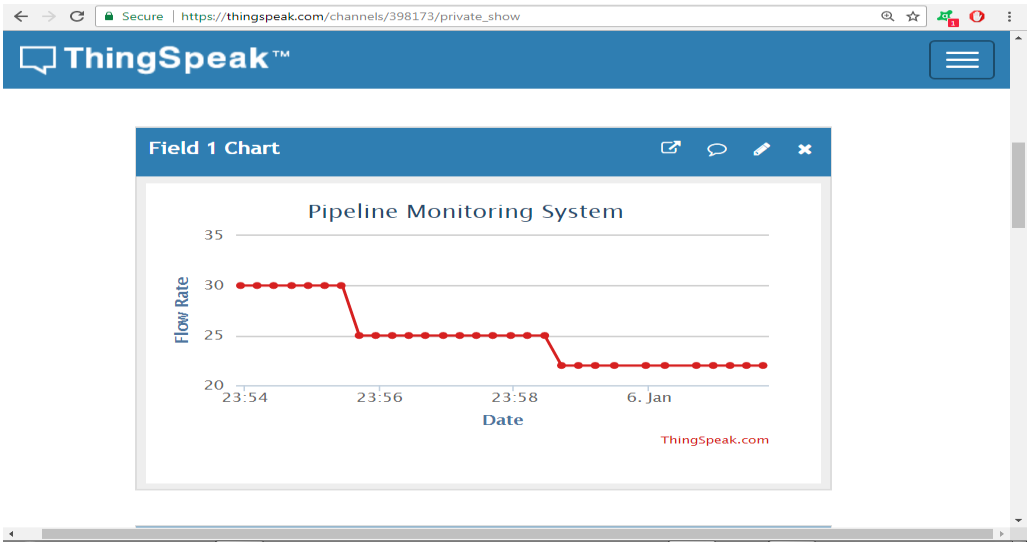

Fig. 5: IoTPMS Flow rate and Intrusion Data.

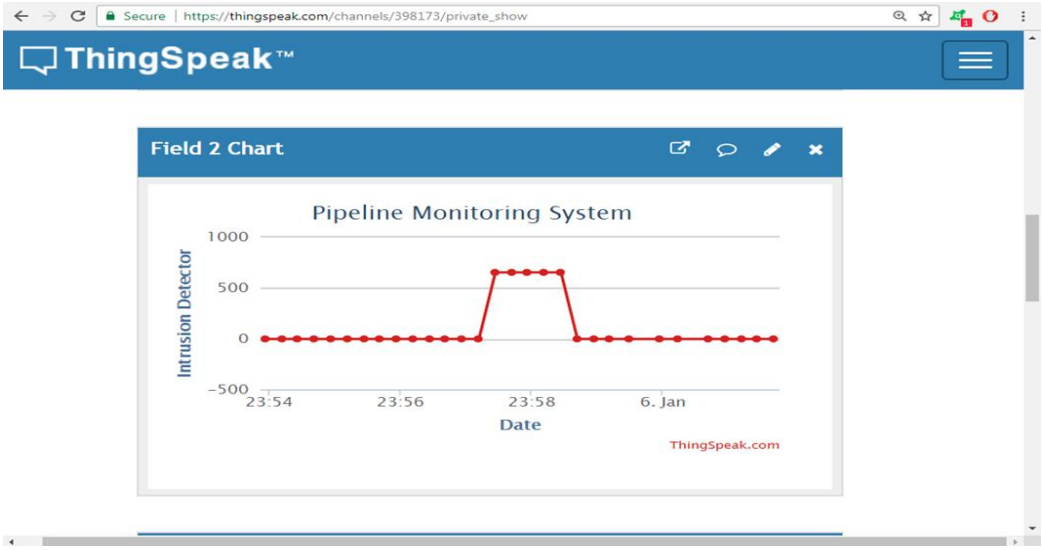

Figure 6: ThingSpeak IoTPMS Channel displaying Intrusion Updates.

With a combination of these data updates, the data analyst can compare data updates between the intrusion detection field and the flow rate field to evaluate the possible cause of drop in flow rate of the fluid flowing through onshore crude oil pipelines.

The drop in flow rate in Fig. 5 from 30 litres/minute to 25 litres/minute between 23:56 (11:56 PM) and 23:58 (11:58 PM) coincided with the detection of an intruder in the intruder detector field chart between 23:56 (11:56 PM) and 23:58 (11:58 PM) in Fig. 6. This means that the drop in flow rate must have been caused by the intruder. The drop in flow rate in the flow rate field chart from 25 litres/minute to 22 litres/minute from 23:58 (11:58 PM) in Fig. 5 did not coincided with the detection of a third-party intruder in the intruder detector field chart in Fig. 6. This means that the drop in flow rate was not caused by an intruder and must have been as a result of material breakdown or failure due to aging, wear and tear, corrosion, extreme weather conditions etc.

These field charts help the data analyst to have the full knowledge of the rate of flow of crude oil through the pipelines and also presence of vandals remotely and in real-time. It also helps in taking proactive actions such as contacting the appropriate authorities informing them of the long-time presence of an intruder on the right of way of pipelines which will aid in the apprehension of the vandals before the intended act of vandalism is carried out. These mechanisms also help in taking corrective action such as informing the pumping station to shut down supply valves for a particular section of the downstream crude oil pipeline network in case of spillage as soon as a drop in flow rate is detected.

Fig. 7 is a screenshot of the IoTPMS ThingSpeak webpage on a web browser showing the Google location map of the IoTPMS prototype. This feature helps in identifying the exact location and coordinates of the affected regions of pipeline networks.

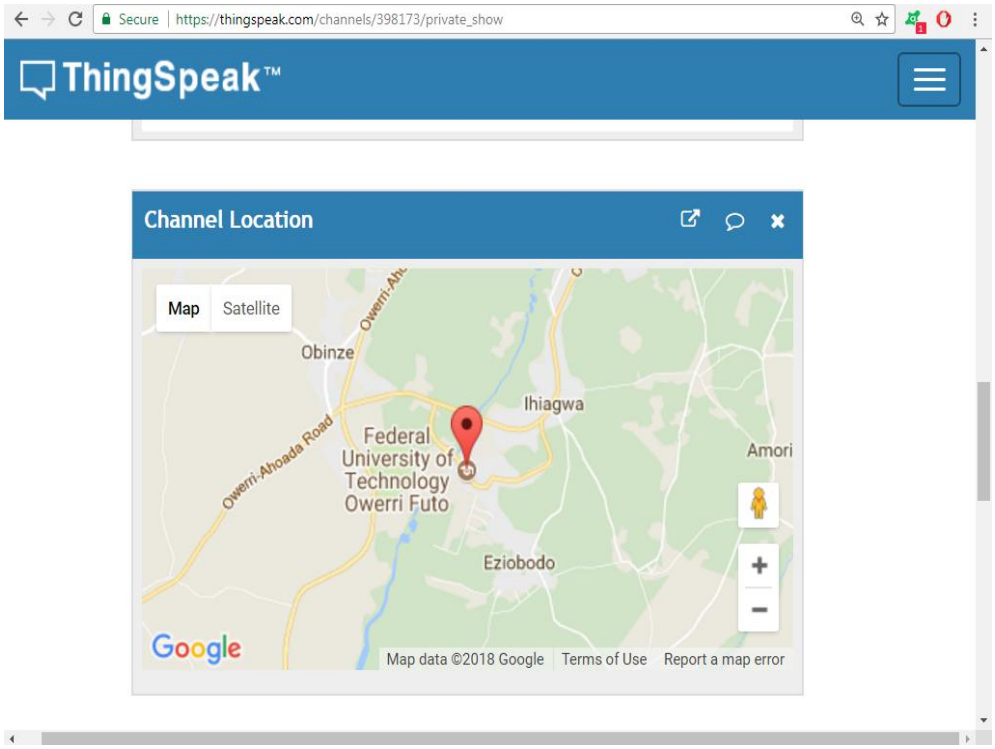

Fig. 7: ThingSpeak IoTPMS Channel showing Google Map location of the device.

CONCLUSION

The role of crude oil pipeline monitoring cannot be overemphasized and onshore crude oil pipeline monitoring systems are necessary in order to complement the efforts of the security operatives that work round the clock to ensure the security of onshore crude oil pipeline networks in Nigeria. The IoTPMS prototype developed in this research is both Green-Field and Brown-Field implementation approach friendly in the sense that it can be incorporated in both existing onshore crude oil pipeline networks and future onshore crude oil pipeline projects. The IoTPMS prototype monitors the flow rate of the fluid flowing in pipelines, intrusion, obtains data as it monitors the flow rate and third-party intrusion and sends the obtained data from the field along with the location every 20 seconds to a secure ThingSpeak Pipeline Monitoring System data analytics channel using a Wi-Fi network for real-time remote monitoring of downstream crude oil pipelines without human intervention thereby making downstream crude oil pipeline networks smart. The IoT capability of the IoTPMS prototype developed in this research work takes care of the problem of real-time monitoring of onshore crude oil pipelines remotely, the problem of delay in transmitting and receiving

data from the field over long distances and it makes data collation, analysis and storage easy. It also makes it easy to troubleshoot the device because the entire system is online and any faulty component of the system would simply stop updating on the data analytics web channel and if the entire system is faulty, it would simply go offline.

Crude oil is not the only product that is transported through pipelines. Refined petroleum products such as kerosene, diesel and premium motor spirit are also transported through pipelines as well as liquefied natural gas. Hence, the concept of the IoTPMS prototype developed in this research can also be deployed for the safety of the pipelines that transport these products.

RECOMMENDATIONS

Further research works on IoTPMS using IoT enabled sensors is recommended.

Attempts to actualize the same goal that this research has achieved through different approaches such as the use of different sensors like the Human Presence Thermal Sensors, embedded modules and different software tools in a bid to make this system better is recommended.

The use of Satellite communication instead of Wi-Fi network for further research works on IoTPMS is recommended.

Only one unit of the Internet of Things Pipeline Monitoring distributed sensing system was developed in this research. Any future work which will deploy as many of the distributed sensing units as possible is recommended.

Only the design, construction and testing of the prototype of the IoTPMS was done in this project. Any future work which will focus on full scale construction and implementation of this design is recommended.

REFERENCE

1. Ezeh, G. N., Chukwuchekwa, N., Ojiaku, J. C. & Ekeanyanwu, E. Pipeline Vandalisation Detection Alert with SMS. *International Journal of Engineering Research and Applications*, 2014; 4(4): 21-25.
2. Igbajar, A. & Barikpoa, A. N. Designing an Intelligent Microcontroller based Pipeline Monitoring System with Alarm, Sensor. *International Journal of Emerging Technologies in Engineering Research*, 2015; 3(2): 22-27.

3. Kachikwu, E. I., Nigeria Records 1,600 Pipeline Vandalism Cases. The Punch Newspaper, 2016, August 18; Retrieved from, https://www.punchng.com/nigeria-records-1600-cases-pipeline-vandalism-kachikwu/. Accessed on March 18, 2017.
4. Obodoeze, F. C., Asogwa, S.C. & Ozioko, F.E. Oil Pipeline Vandalism Detection and Surveillance System Niger Delta Region. *International Journal of Engineering Research & Technology*, 2014; 3(7): 156-166.
5. Ononiwu, G. C., Eze, P. U., Onojo, O. J., Ezeh, G. N. & Dike, D. O. A Real-Time Oil Pipeline Anti-Intrusion System Using Acoustic Sensors. *British Journal of Applied Science & Technology*, 2014; 4(26): 3740-3756.
6. Organization of Petroleum Exporting Countries (OPEC). OPEC Annual Statistical Bulletin [PDF], 2016; Retrieved from https://www.opec.org/opec_web/static_files_project/media/downloads/publications/ASB2016.pdf. Accessed on January 18, 2017.
7. Organization of Petroleum Exporting Countries (OPEC). Annual Statistical Bulletin, 2017; Retrieved from http://www.opec.org/opec_web/en/about_us/167.htm. Accessed on September 23, 2017.
8. Shoewu, O., Akinyemi, L. A., Ayanlowo, K. A., Olatinwo, S. O. & Makanjuola, N. T. Development of a Microcontroller based Alarm System for Pipeline Vandals Detection. *Journal of Science and Engineering*, 2013; 1(2): 133-142.