

EDGE GATEWAYS AS A MEANS TO STREAMLINE COMMUNICATIONS BETWEEN DEVICES AND THE CLOUD

Professor Francisca Ogwueleka
Dept. of Intelligence and Cybersecurity
Nigerian Defence Academy, Kaduna
franciscaogwueleka@nda.edu.ng

Nnamdi Judges Ajah
Dept. of Mechanical Engineering
Nigerian Defence Academy, Kaduna
jannamdi@nda.edu.ng

ABSTRACT

The proliferation of sensors, cloud computing, real-time data analysis, and convergence of embedded hardware with software has been driving a new revolution - Internet of Things (IoT). Because of the lack of a unified standard for IoT, many of the current IoT solutions provide issues. These issues lead to many problems such as inability of solutions to scale, rigidity of solutions, vendor lock-in etc. which have prevented many from adopting the technology and inhibiting the growth of IoT. To overcome these challenges and enable resource sharing among devices with different communication interfaces and data formats, an edge gateway is proposed. An edge gateway acts as a bridge between sensors/devices over varying protocols and then translates that data into a standard protocol to be used for communication between devices and the cloud.

Keywords: Edge gateway, Internet of Things, protocol, cloud, sensors

1. INTRODUCTION

Internet of Things (IoT) is a network of devices connected to the internet (Dave, 2011). It was only in the last few years that IoT was a buzzword. Today, IoT has entered the mainstream and continues to grow in impact and market share. According to a report, the number of IoT devices were predicted to surpass the number of mobile phones in 2018 and an estimated total of 75.44 billion IoT devices will be installed globally by 2025 (Ericsson, 2016). This growth is largely driven by the global adoption of cloud platforms, big data, and artificial intelligence, with IoT acting as the eyes and ears of the world (Zion Market Research, 2019).

A consequence of the growth of IoT is the heterogeneity of connected things. IoT spans across an abundance of industry verticals that include healthcare, agriculture, commerce, energy, utilities, transportation etc. and each of these verticals have their unique requirements. As a result, there is a multitude of languages, protocols and standards, as well as a lack of agreement on the best implementation of IoT. This problem is going to be compounded by the projected growth in smart cities, smart factories, connected cars, and machine-to-machine communication, thereby, necessitating valid calls for IoT interoperability in order to maximize the benefits for these ecosystems (Don, et al., 2017; Gilchrist, 2017).

The resulting effect of the numerous and different closed IoT ecosystems is that customers are going to be bound to the specific device, and/or software offered by their provider, else, risk paying a high switching cost (Unify IoT, 2015). The incompatibility between the various systems promoted by service providers and Original Equipment Manufacturer OEMS, also means that IoT developers would have to adapt their solution to the platform specific hardware, API and information models (Macaulay, 2016). This makes both the IoT developer and owner of the solution to run at a risk, a risk of not being able to integrate into other systems, and scale.

Increasingly, there are calls to solve the interoperability challenges in IoT. Attempts to solve this problem has been through standardization. To accelerate the standardization process, the European Union recently funded several research projects under the H2020 program focusing on the federation of IoT platform (European Commission, 2019). This is in addition to the list of innovative solutions being developed by researchers in industry and academia. Nonetheless, it will take quite a while before related standards are fully agreed on and accepted.

2. REVIEW OF LITERATURE

IoT systems require interoperability among devices, applications, and the cloud to function seamlessly. The lack of standards for IoT and the competing ecosystems built by competing vendors make interoperability difficult (GSM Association, 2016). This has been causing lots of concern, as such lots of research efforts are ongoing to solve it. To solve some of the challenges with data device and application interoperability, some researchers developed a software framework based on patterns of interoperability behaviour to solve semantic communication issues (Paul, et al., 2014). They were able to convert various message data type (e.g. JSON, csv etc) from different devices into a single message data type for ingestion into the cloud. While, this solves one aspect of the problem, it overlooked the problems of incompatible Application Programming Interfaces

(APIs) among IoT devices. This is because of the walled ecosystems built by various cloud vendors. To enable interaction between various internet services used by devices, researchers proposed the development of a common and simplified API management layer to enable communication (Venkateswara & Bharamagoudra, 2017).

Middleware has also been promoted as a way of solving interoperability between new services and applications. The use of a software middleware through the integration of the Calvin framework, MQTT protocol, and Open Connectivity Foundation (OCF) data model was found to provide interoperable and dynamic communication between devices in a smart home and the online application layer (Fernanda, et al., 2019). However, all the devices must use JSON message data type, and communicate via Message Queuing Telemetry Transport (MQTT) over a Transmission Control Protocol/Internet Protocol (TCP/IP) connection.

Because of the merging of different systems, and the complexity involved, some researchers suggest that IoT architecture, and network infrastructure needs to be rebuilt from the ground up: so that IoT solutions can be safely and efficiently deployed (Shariq, et al., 2017). The unique interaction among IoT devices in a certain segment such as health has led researchers to suggest the use of specific standards for specific industries. Researchers proposed a framework for achieving high interoperability amongst devices and the cloud in healthcare (Argyro, et al., 2019). Likewise, Jun Choi has advocated for the use of different IoT standards for different industries (Jun, 2016).

Going through the literatures, it is observed that most of the models proposed for solving interoperability issues in IoT systems are software based. While they are able to solve the semantic, and syntactic issues among IoT platforms, they are leaving out the hardware communication interoperability problem. This paper suggests a framework to solve both the hardware communication, and software interoperability issues in IoT systems. Therefore, the subsequent sections talk about the various interoperability domains, before talking about the edge gateway architecture.

3. INTEROPERABILITY

IoT deployments would continue regardless of the lack of standardization. A key concept, Edge Gateways that has enabled cross-interaction among devices, and cloud platforms in IoT shall be discussed. To enable better understanding of Edge Gateways, it is important to first get an understanding of interoperability in the three IoT taxonomies: hardware, software, and the cloud.

3.1 IoT Interoperability

Interoperability simply means the ability to operate in conjunction. To understand IoT interoperability, we would need to approach it according to the three broad components that make up an IoT system, namely the hardware, software, and the cloud (Happ, 2017)

3.2 Hardware Interoperability

IoT systems are usually composed of a variety of devices. These devices called “Things” in the “Internet of Things” is a processing unit that is capable of connecting to the internet and exchanging data with the cloud (Daniel, 2019). They include sensors, micro-controllers etc. The definition of a device is usually dependent on the project. There may be times when a device may be considered as a separate entity, and other times when a group of sensors and equipment are considered as a single device (Microsoft, 2018). The characteristics of these devices such as the communication technology, processor speed, ram, and battery differ broadly between different brands and models.

For example, Arduino micro-controllers support both digital and analog signals, are usually not equipped with WiFi technology. While, Raspberry Pi supports only digital signals and all their models come equipped with WiFi technology. More recently, IoT devices for medical usage are based on Bluetooth LE. Home devices such as TVs, adapters, refrigerators etc. use WiFi technology. On the other hand, most payment systems and vending machines are mostly based on Bluetooth 4.2 and near field communication, while different ambient and farm sensors use Zigbee based communications.

Apparently, all of these devices do not speak the same language of communication. Hence, there is difficulty in exchanging information between these variegated devices and enabling them to work seamlessly together.

3.3 Software Interoperability

Different hardware for IoT have their own unique programming language. For instance, an Arduino is usually programmed with C, while Raspberry Pi with python. And because there is usually no de-facto agent, services, and data processing format for these devices, there are usually syntactic and semantic issues.

Syntactic issues usually arise as a result of conflicting interfaces such as REST APIs used in the exchange of information between heterogeneous IoT system entities. The resource owner (a platform, software, database etc.) encodes data in a message using syntactic rules, specified in some grammar that is incompatible with the decoding rules of the device trying to access the resource.

Semantic issues usually arise when data generated by devices are in a defined data format (e.g. JSON, CSV, CBOR), but the data models and schemas used by other entities on the IoT network are usually dissimilar and not always compatible. Sometimes, the data may be in a different unit of measurement, or be operating according to a different time zone. As a result, different entities of an IoT system may not be able to operate together in harmony as they have different descriptions or understandings of resources and operational procedures.

3.4 Cloud Platform Interoperability

Cloud platform interoperability issues in IoT arises due to the increasing number of diverse cloud platforms. IoT cloud provider list includes Amazon AWS IoT, Azure IoT Hub, Google’s Cloud IoT Core, Temboo, Thingspeak etc., and each of these providers offer their own SDKs and different brokered communication model. Not until recently when Google introduced Anthos, a hybrid cloud, there was no easy way to deploy, monitor, and migrate solutions across cloud platforms.

The different brokered communication across these cloud platforms restricts IoT developers to develop and/or integrate cross-platform IoT applications. Once an IoT solution is connected to a particular cloud platform, there’s usually vendor lock-in, as the vendor may not provide the capability to have data pipelines to services of other cloud solution providers. This makes it difficult for IoT developers to migrate their solutions to other cloud platforms or integrate services such as data warehousing or computation from other cloud providers.

4. EDGE GATEWAYS, A SOLUTION?

Gateways are devices that act as bridges between sensors/devices and the cloud (Daniel & Adam, 2017). While sensors/devices can talk directly to the cloud, gateways can be used to facilitate the communication. They are different from routers in the sense that they have an active role in managing access and information flow. Edge gateways essentially sit between the cloud and IoT endpoints (devices) in the field, and can be used for a variety of different tasks, including preparing data for transmission to the cloud. Also, they are capable of aggregate data from different devices, processing the data, batching and aggregation, buffering of data, protocol translation, and even perform localized machine learning inferencing (Peter, et al., 2019).

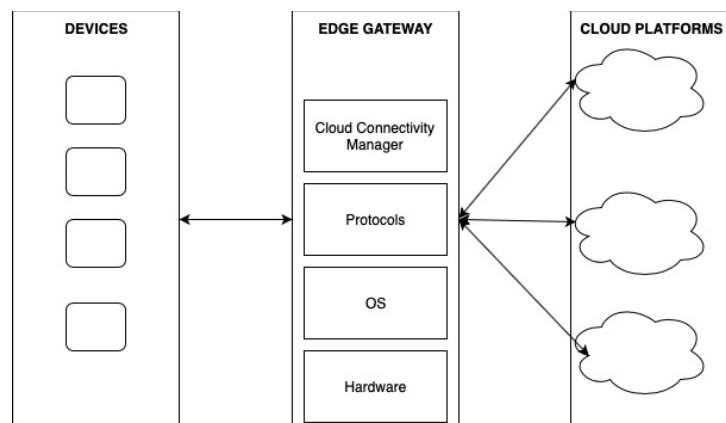


Figure 1: IoT Architecture with Edge Gateway

4.1 IoT Edge Gateway Architecture

From Figure 1, it can be seen that the IoT devices do not connect to the cloud directly. Instead, they connect through an intermediary i.e. the Edge Gateway. The edge gateway then handles the interaction between the IoT devices and the cloud by converting the messages into the format and protocol required for transmission. When devices also need to talk to each other, the sender sends its message to the other device through the Edge Gateway. The Edge Gateway then converts the message into the format and protocol required by the receiving device and delivers the message to the recipient.

To enable bi-directional communication between devices, and the cloud, IoT Edge Gateway should consist of several building blocks. The hardware and operating system are the primary building blocks of edge gateway. The hardware is usually an embedded system designed around a core computing module that contains the CPU, memory, networking, and other core components. The hardware also provides an interface for various sensor supports such as Modbus, Profibus, I2C etc. by having ports for connectivity, and also to enable interaction with peripherals such as USB devices.

To run the hardware, an operating system is usually necessary. The complexity of the tasks and hardware are usually what determines the selection of the operating system. The operating system also enables hardware abstraction layer, which essentially supports portability and reusability of IoT software components. This allows different hardware drivers to support

communication with various hardware. The operating system is also responsible for providing an application framework to provide services API for applications that will run on the operating system.

The Edge Gateway enables data communication with the internet over ethernet, Wi-Fi, Bluetooth, or cellular connectivity. On the operating system is a software stack for establishing communication with the internet for data exchange. It provides support for various communication protocols such as https and mqtt.

An essential part of the Edge Gateway is support for Cloud Connectivity Manager. This is also a function provided by the software, and it enables parallel interaction with various cloud platforms. Therefore, the Edge Gateway as the capability send an receive requests from various cloud platforms concurrently. Among the tasks that it can perform includes reconnection when connectivity is lost, monitoring of device state, and identity access management with the cloud.

4.2 Benefits of Using an Edge Gateway

Using edge gateways as an architectural component in IoT systems provide the following benefits,

- i. **Harmonizing varying protocols:** As mentioned earlier, IoT systems are usually composed of various devices that may have varying rules and format for communication and information exchange. Edge gateways can communicate with these devices over their varying protocols and translate the data into a standard protocol to be sent to the cloud (David, 2019). Likewise, when information is sent from the cloud to field devices, the edge gateway can translate the information into the required data format and protocols required for the devices.
- ii. **Filtering Data:** The data that sensors/devices generate can sometimes be overwhelming. To transmit this data may be costly and may take up precious storage. The data being generated can be pre-processed by gateways in order to send only data that is valuable, thereby decreasing transmission, processing, and storage requirements (Tamas & Attila, 2018). For example, the gateway can find the average value of temperature sensors spread across a hallway and transmit that information, as opposed to sending the individual values of each temperature sensor.
- iii. **Low Latency:** Time may be of importance to some IoT applications. A monitoring system for a life-support equipment may not afford to transmit data to the cloud and wait to get a response before acting. A gateway can act to reduce the latency by drawing an inference locally and giving control commands, this way time is reduced by the gateway performing the processing instead of it being sent to the cloud (Amir, et al., 2019).
- iv. **Hybrid Communication across Clouds:** Edge gateways are capable of communicating with different cloud endpoints, and aggregating information from them. They can therefore be used to pull a resource from a cloud service and push it to a service on another cloud provider. In addition, they can ensure that data from various sensors can be to the desired cloud providers. For example, a gateway can take data from sensor A and push it to a cold storage service on a cloud provider, while sending data for hot storage to another cloud provider for cost reasons.
- v. **Security:** Because gateways act as the layer between sensors on the field and the internet, it reduces the number of devices exposed to the internet, because the sensors/devices are only connected to the gateways. Managing the security for only one device (the gateway), is far easier than managing security for a plethora of devices (Manuel, et al., 2017).

5. CONCLUSION

IoT solutions should be capable of scaling connectivity of devices, and interoperability across platforms. With the expansion of IoT systems, there is an increasing need to ensure seamless operation among various IoT entities, and the ability to integrate new devices on an IoT network. To meet this need, incorporating edge gateway on an IoT solution is recommended. This is because it enables for the decoupling of sensors/devices from the cloud and facilitates more robust communication between them.

6. REFERENCES

- [1] Amir, K., Abdelhakim, H. & El-Mostapha, A. (2019). *On the Fog-Cloud Cooperation: How Fog Computing can address latency concerns of IoT applications*. Rome, IEEE.
- [2] Argyro, M., Athanasios, K., Konstantinos, P., Stamatios, P., & Dimosthenis, K. (2019). IoT in Healthcare: Achieving Interoperability of High-Quality Data Acquired by IoT Medical Devices. *Sensors (Basel)*, pp. 1978-1985.
- [3] Daniel, H. & Adam, W. (2017). *Towards gateway to Cloud offloading in IoT publish/subscribe systems*, Valencia: IEEE.

- [4] Daniel, K. (2019). *Connecting IoT Devices with Sensors to the Azure Digital Twins*. Apress, 24 August, pp. 3-20.
- [5] Dave, E. (2011). *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*, Vancouver: Cisco Internet Business Solutions Group (IBSG).
- [6] David, J. (2019). *Azure DevOps for IoT Edge Solutions*, Berkeley: Springer Link.
- [7] Don, D., Emil, B. & Wael, E. (2017). *The Future of IoT: Leveraging the Shift to a Data Centric World*, New Jersey: BookBaby.
- [8] Ericsson. (2016). *Ericsson Mobility Report*, Stockholm: Ericsson.
- [9] European Commission. (2019). *Research & Innovation in Internet of Things*. [Online] Available at: <https://ec.europa.eu/digital-single-market/en/research-innovation-iot> [Accessed 5 October 2019].
- [10] Fernanda, F., Cleuves, C., Danilo, S., Angelo, P., & Kyller, G. (2019). *Dynamic and Interoperable Control of IoT Devices and Applications based on Calvin Framework*. Campina Grande, Embedded Lab, Federal University of Campina Grande, pp. 7-23.
- [11] Gilchrist, A. (2017). *IoT Security Issues*, Nonthaburi: De Gruyter.
- [12] GSM Association. (2016). *GSMA IoT Connection Efficiency Guidelines*. [Online] Available at: <https://www.gsma.com/iot/gsma-iot-device-connection-efficiency-guidelines/>
- [13] Jun, C. (2016). *Issues for IoT Interoperability*. ITU, pp. 1-40.
- [14] Manuel, S.-A., Tiago, M. F.-C., Paula, F.-L. & Luis, C. (2017). *A Practical Evaluation of a High-Security Energy-Efficient Gateway for IoT Fog Computing Applications*. Coruna, MDPI.
- [15] Microsoft. (2018). *Microsoft Azure IoT Reference Architecture*, Redmond: Microsoft.
- [16] Paul, G., Justan, B., Brian, P. & Mike, S. (2014). *Taming the Interoperability Challenges of Complex IoT Systems*. Bordeaux, Association for Computing Machinery.
- [17] Peter, P. et al. (2019). *Edge-enabled IoT gateway criteria selection and evaluation*, s.l.: Wiley Online Publication.
- [18] Shariq, H., Aisha, H., Othman, K. & Ahmad, F. (2017). *Connectivity, Interoperability and Manageability Challenges in Internet of Things*. Maryland, AIP Publishing, pp. 101-124.
- [19] Tamas, P. & Attila, K. (2018). *A Private Gateway for Investigating IoT Data Management*. Madeira, Scite Press.
- [20] Unify IoT. (2015). *Report on IoT platform activities*, Paris: European Platform Initiatives.
- [21] Venkateswara, R. K. & Bharamagoudra, M. R. (2017). *Challenges and solutions of interoperability on IoT: How far have we come in resolving the IoT interoperability issues*. Bangalore, IEEE.
- [22] Zion Market Research. (2019). *Global Share of IoT Devices Market Size Will Reach USD 158,140 Million by 2024*, New York: GlobeNewswire.

Author's Brief Profile



Francisca Nonyelum Ogwueleka is a Professor of Computer Science and Cyber Security in Nigerian Defence Academy, Kaduna-Nigeria. Her research focuses on big data, artificial intelligence, cloud security, data mining techniques, steganography, penetration testing solutions and information security. She has nine published books, two book chapters and ninety-five original articles in international and national journals. She is an external examiner for PhD dissertation and M.Sc thesis evaluation for national and international universities. She was a resource person for the development of Nigeria Undergraduate Curriculum in Cyber Security and Information Technology programmes for National Universities Commission.



Nnamdi Ajah holds a Bachelor of Engineering (B.Eng) and Master of Engineering (M.Eng) degrees from the University of Nigeria, Nsukka, and Nigerian Defence Academy, Kaduna respectively. His research areas include Energy, and Smart Grid Systems. He can be reached on phone through +2348164187604, and by email with jannamdi@nda.edu.ng