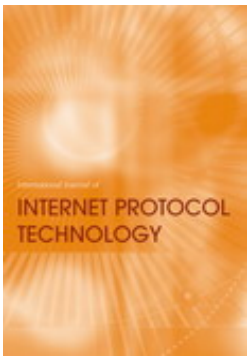


International Journal of Internet Protocol Technology

ISSN online: 1743-8217 - ISSN print: 1743-8209
https://www.inderscience.com/ijipt

Design and implementation of internet protocol system: application for the IoT platform

A. Rajalingam, S.R. Balaji, D. Chitra Devi, Sheshang Degadwala

DOI: 10.1504/IJIPT.2024.10067599

Article History:

Received:	07 December 2023
Last revised:	26 April 2024
Accepted:	08 June 2024
Published online:	06 January 2025

Design and implementation of internet protocol system: application for the IoT platform

A. Rajalingam

Department of Electronics and Communication Engineering,
University of Technology and Applied Sciences,
Shinas, Oman
Email: Raja.lingam@utas.edu.om

S.R. Balaji

Department of Electronics and Instrumentation Engineering,
Panimalar Engineering College,
Chennai, Tamil Nadu, India
Email: balasrb2000@gmail.com

D. Chitra Devi

Department of Computer Science and Engineering,
S.A. Engineering College,
Chennai, Tamil Nadu, India
Email: chitradanya@gmail.com

Sheshang Degadwala*

Department of Computer Engineering,
Sigma Institute of Engineering,
Vadodara, Gujarat, India
Email: sheshang13@gmail.com
*Corresponding author

Abstract: Virtual objects are quickly becoming an integral component of all Internet of Things systems, and this trend is expected to continue. When something exists in the physical world, it is referred to as a virtual item. A virtual item is the digital version of that object. The Internet of Things platform that is being proposed is different from others that are currently in existence since it provides clients with the opportunity to plug and play both hardware and software services on a single platform. A user interface that is easy to understand has been proposed for the Internet of Things platform. Other features include reliability and security. By using virtual objects, it is possible to complete the tasks of monitoring and controlling Internet of Things devices. As part of a side-by-side comparison that we carried out, the Internet of Things platform that was recommended was tested alongside FIWARE.

Keywords: IoT; internet of things; CoT; cloud of things; Amazon elastic compute cloud; EC2; IoT marketplace; IoT platform; Raspberry Pi; virtualisation.

Reference to this paper should be made as follows: Rajalingam, A., Balaji, S.R., Devi, D.C. and Degadwala, S. (2024) 'Design and implementation of internet protocol system: application for the IoT platform', *Int. J. Internet Protocol Technology*, Vol. 17, No. 1, pp.9–18.

Biographical notes: A. Rajalingam works in the Department of Electronics and Communication Engineering at University of Technology and Applied Sciences, Shinas, Oman.

S.R. Balaji currently works in the Electronics and Instrumentation Engineering at Panimalar Engineering College, Chennai, India.

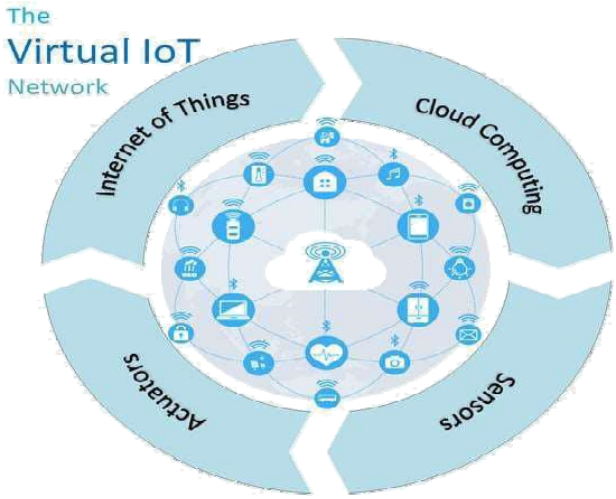
D. Chitra Devi works in the Department of Computer Science and Engineering, S.A. Engineering College, Chennai, India.

Sheshang Degadwala is presently working as an Associate Professor and the Head of Computer Engineering Department, Sigma Institute of Engineering, Vadodara. He obtained his BE degree from the Department of Computer Engineering, BITs, Vadodara. Subsequently, MTech degree from the Charusat University, Changa and PhD degree in Computer Engineering from the Madhav University, Abu Road, Sirohi, Rajasthan, India in 2018. He has published 179 research papers in reputed international journals and conferences including IEEE, Elsevier and Springer. He is also a Microsoft Certified in Python Programming and Excel. He has published 18 books and he got grant for one patent. He has published 38 Indian patents. He has received 45 awards for academic and research achievement.

1 Introduction

Many as 50.6 billion linked gadgets in use by the year 2020 (Lee et al., 2017), according to estimates. The Internet of Things (IoT) is made up of commonplace things like electrical gadgets, buildings and automobiles that are equipped with embedded software, electronics, sensors and network connection and have the ability to gather and share data with one another. The development of a virtual Internet of Things network is shown in Figure 1, which depicts the various technologies involved. The Internet of Things is independent of human-to-machine or human-to-human contact, therefore it may send data across a network without the need for any of those. The Internet of Things is a very important component in many various industries, including finance, education, healthcare and smart cities (Park et al., 2018; Wu et al., 2018). Temperature, humidity, pressure, motion and heat sensors are some of the varieties of sensors that may be purchased on the market today. Actuators are used to conduct a particular action in response to the data collected by the sensors. The Internet of Things not only detects and processes data, but it also triggers the operation of a variety of devices depending on the dynamics of the data. The Internet of Things relies on a mix of sensors and actuators to power its automation.

Figure 1 Convergence and evolution of network technology

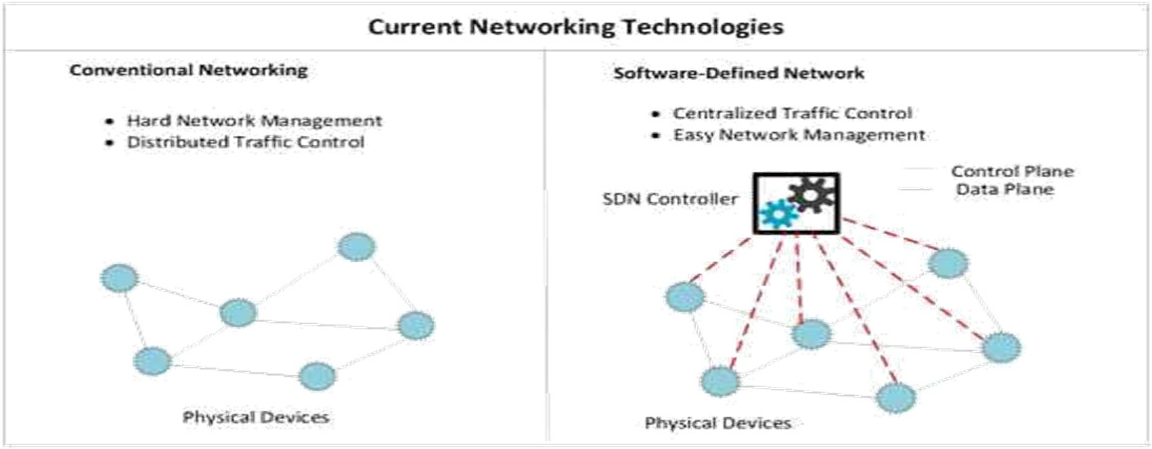


The Internet of Things creates an enormous volume of large data, which places an incredible strain on the internet's underlying infrastructure (Kharrazi et al., 2016). Cloud computing is an extremely important component in managing data storage. Cloud computing has the potential to lessen the strain placed on the infrastructure of the internet. Cloud computing, in its most basic form, refers to the act of drawing one's data and software applications from a shared repository of computer resources. Cloud computing and the internet of things have a connection that is mutually beneficial, and both aim to improve the effectiveness of routine activities (Ferrández-Pastor et al., 2018; Cirani et al., 2018). The Internet of Things creates a tremendous quantity of data, and cloud computing makes it possible to store the data and perform computations on it. The use of cloud computing also allows for improved fraternisation, which is an essential skill for software engineers.

Despite the fact that their primary purpose is to facilitate communication between machines, sensors and controllers. M2M is an umbrella term for a variety of technologies that, when combined, make it possible for endpoint devices to communicate with one another without the intervention of a person. M2M stands for machine-to-machine communication, while IoT takes M2M connectivity and adds web application integration in addition to connecting it to the cloud. M2M serves as the basis for the Internet of Things. M2M makes use of individual networks of sensors, but the Internet of Things integrates previously separate networks into a single expansive network to facilitate the development of new applications. Because it is built on cloud computing, the Internet of Things is more scalable than M2M. It is more accurate to say that the Internet of Things is a network of things that are connected to one another (Mehmood et al., 2019; Jamil et al., 2019; Fremantle, 2015; Stewart et al., 2017). The Internet of Things incorporates more than simply the connecting of physical objects.

In Section 6, the findings of the experiment are presented. In Section 7, you will find the discussions. In the last section of the study, entitled 'Conclusion', a view on our future work is presented (Voulvoulis et al., 2017; Montginoul and Vestier, 2018).

Figure 2 Present network tech



2 Related technologies

2.1 LPWAN

The transmission of tiny quantities of data is required (Raza et al., 2017). This was previously discussed in the part that was dedicated to the introduction. In contrast to WiFi, Bluetooth, ZigBee and NFC, it is capable of supporting connections over a wider distance, and its scalability is better as a result of its capacity to handle a bigger number of devices (Khutsoane et al., 2017).

NB-IoT is a Low-Power Wide-Area Network (LPWAN) technology that was developed and standardised by the 3rd Generation Partnership Project (3GPP). This technology makes use of the licensed frequency bands that are allotted to mobile phone carriers and makes use of the infrastructure that is already in place. Disadvantages include a shorter range and the fact that LTE coverage is not available in all suburban areas (Mekki et al., 2018).

The academic community. Both use radio frequencies designated as ISM, which stands for 'Industrial Scientific and Medical.' If the radiated power, bandwidth and transmission cycle limits are satisfied, it is feasible to operate in the ISM bands without the need for a license. However, this is only the case if the ISM bands are used. The 868 MHz band, as established in the ECC 70-03 (European Research Council, 2018), is the one that these technologies use the most often in Europe.

2.2 Sigfox

In addition to being the name of a technology that is used for the Internet of Things, Sigfox (SIGFOX Company, 2018) is also the name of a network operator that provides a solution that is all-encompassing. The first thing that has to be done in order to implement this solution is to gather data from objects that are situated in any region of the world that is within the boundary of the coverage area. Transmitting this data to the information system of any potential customer is the next step that has to be taken. The concept of the company revolves on the idea of billing customers for the connection services that are provided to their various electronic gadgets. As of the month of November 2018, Sigfox is accessible in 53 countries and is predicted to have a coverage area of 5 million square kilometres (Sigfox, 2018). Since 2009, the company has seen enormous development, and as of this month, it is accessible in 53 countries. The name 'Sigfox' refers to a worldwide network that links various gadgets to the internet. At the present, each base station has a range that is between 3 kilometres and 10 kilometres in urban settings and between 30 kilometres and 50 kilometres in rural settings. Additionally, they are able to provide a variety of services to as many as 1 million devices (Centenaro et al., 2018).

A Sigfox device must first finish a certification process that is defined in the official specifications of Sigfox before it can be registered in the network. This requirement must be met before the device can be registered (Sigfox Build, 2018; Do et al., 2014; Lauridsen et al., 2017). The purpose of this procedure is to ensure that the device and the network are compatible with one another and that a high level of service is maintained.

The downlink frame shown in Figure 4 has the capacity to store up to 8 bytes of user-defined data, although the exact amount depends on the application.

Figure 3 Uplink data-link frame. Fields and associated length

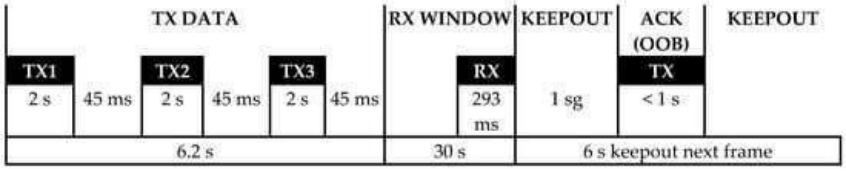


Figure 4 Data-link downlink: fields and length

PREAMBLE	FRAME SYNC	ECC	PAYLOAD	AUTHENTICATION HASH	CRC
91	13	32	0-64	16	8

Figure 5 LoRa/LoRaWAN layer model

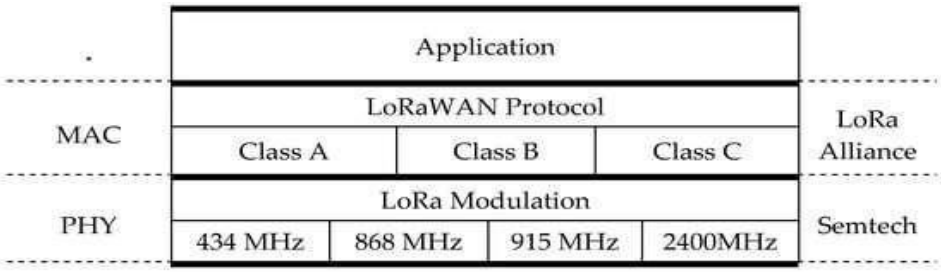


Figure 6 UplinkingLoRaWAN frames and fields

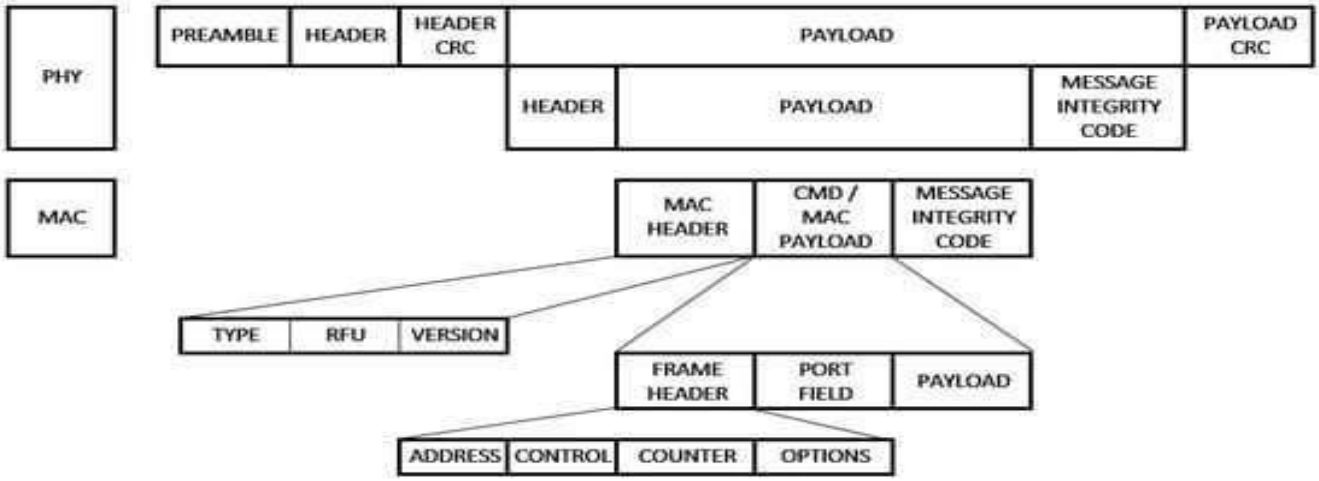
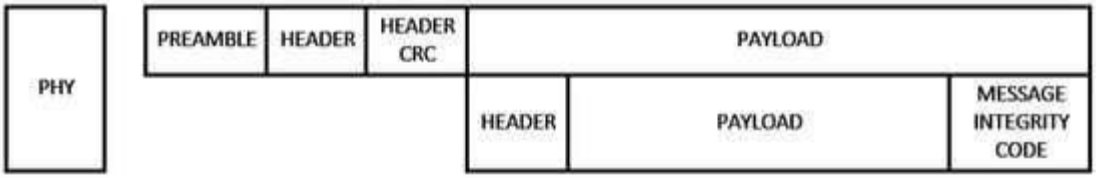


Figure 7 The frame and fields of the LoRaWAN transmission



For reasons of safety, the device identification is used to validate the authenticity of the emitter, and the message's sequence number is used to validate the authenticity of the message. The idea of a cooperative network is put into practice here. In a practice referred to as 'spatial diversity', there are often three base stations covering each zone. Increasing the dependability of message receipt by covering each item with three base stations that are located in three separate places.

There are stated to be three distinct types of technological implements:

- *Class A*: They spend the vast majority of their time in an energy-saving mode. After the information has been sent, they go back to the standby position and maintain two receiving windows.

The payload has a maximum size that may range anywhere from 51 to 222 bytes, depending on the SF and whether it is being sent in the uplink or the downlink 32-bit. DevEui is a 32-bit identifier that is unique to each and every device and is permanent. LoRaWAN incorporates security and authentication measures that are founded on the Advanced Encryption Standard 128-bit AES128 encryption method as well as other security requirements that are outlined in IEEE 802.15.4/2006. Authentication and encryption are handled independently by LoRaWAN, in contrast to other systems which rely on a single key to perform both operations.

3 System architecture of the IoT AP

This section gives an explanation of the system architecture of the proposed Internet of Things Access Point (IoT AP), which is referred to as the comprehensive system architecture in Sub-section 3.2. This particular section may be found in the section that comes after Sub-section 3.1.

3.1 Functionality of the internet of things AP

Figure 8 illustrates the application scenario of the Internet of Things network Access Point (AP) for smart living. A traditional access point that enables different network protocols to interact with one another in order to facilitate communication. This is due to the fact that the traditional access point is not intended to function in this manner. When it comes to the development of a life that is intelligent for the future, it is absolutely necessary to find a solution to the issue of heterogeneous networks.

3.2 IoT AP system architecture

The application platform for the Internet of Things that has been given is integrated with the technologies that are now being used in applications for the Internet of Things smart home. ZigBee, Wi-Fi and Ethernet are the three separate ways of communication that the Access Point for the Internet of Things (IoT AP) provides to users inside the heterogeneous network.

Figure 8 Using IoT for smart life (see online version for colours)

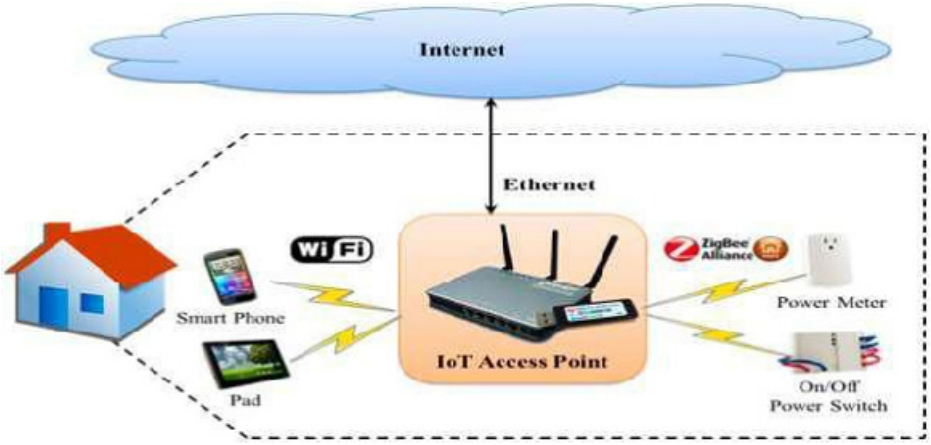


Figure 9 System architecture of the proposed IoT AP (see online version for colours)

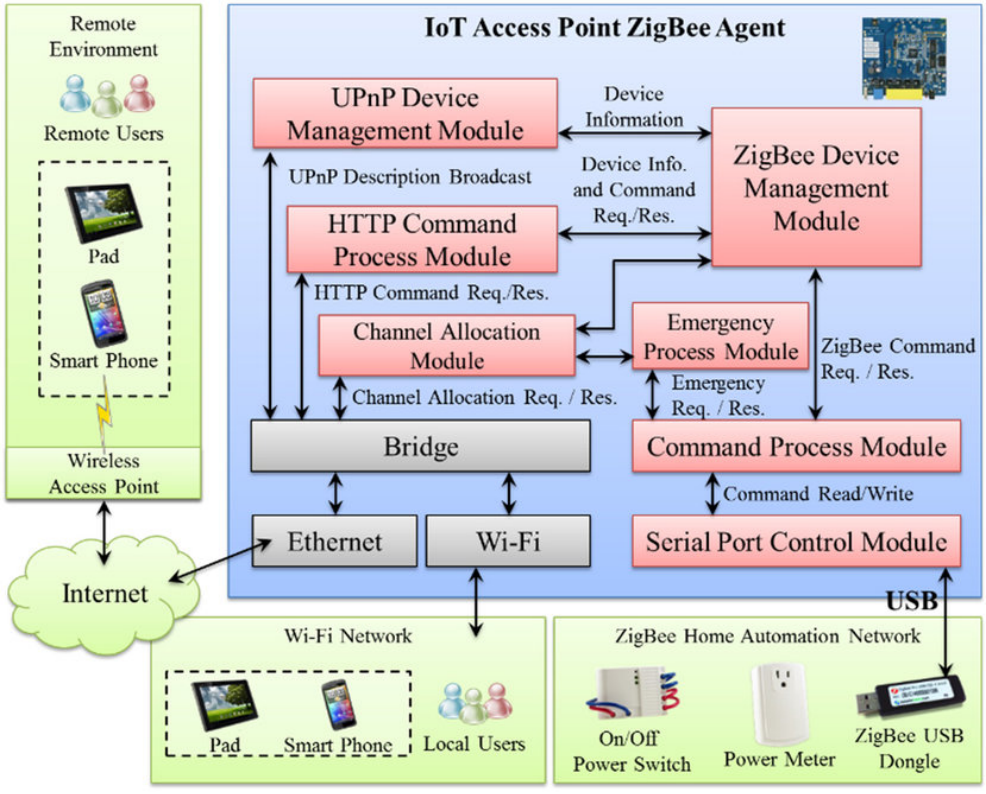


Figure 10 System architecture for ZigBee agent (see online version for colours)

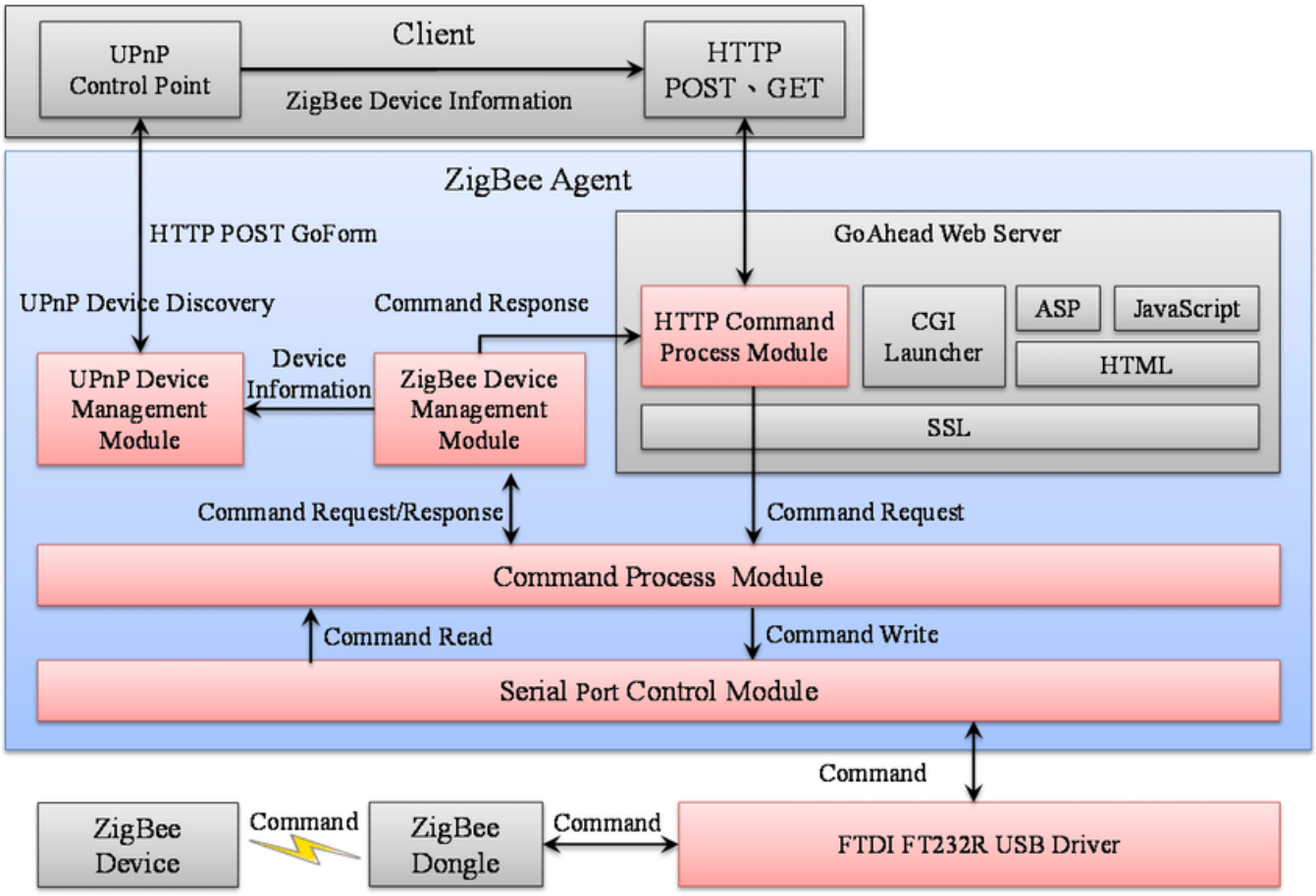
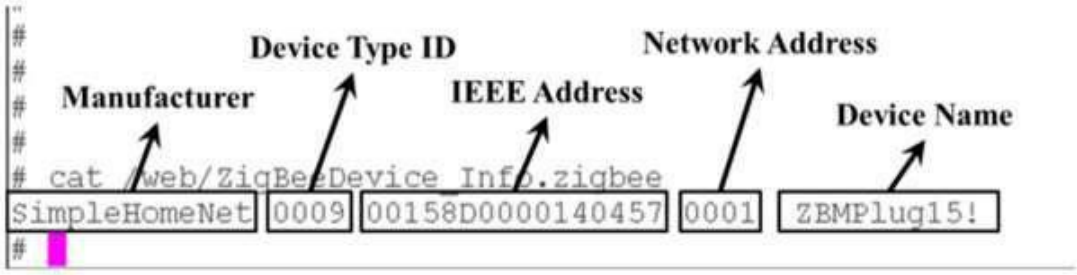


Figure 11 ZigBee device management instructions. The pink dot indicates Linux's CLI mode, where you input commands



4 IoT AP system implementation

A USB transceiver and a ZigBee device are able to communicate with one another via the use of an intermediate device known as a ZigBee agent. The ZigBee control service is made available to consumers over the Internet and is provided by the ZigBee agent that is connected to the ZigBee device. Installing Linux on an RT3052 development board allows us to create a ZigBee agent that is based on the operating system. The system architecture of the ZigBee agent that was developed is depicted in Figure 10.

4.1 ZigBee device management module

As a result of its capacity to manage numerous ZigBee devices concurrently, the Command Process Module makes it possible for the ZigBee agent to manage several ZigBee devices at the same time. In response to a command from the user, this module will first gather the information that belongs to the necessary ZigBee devices, and then it will convert each of those pieces of information into a particular streaming format that is made of several fields. This process will take place sequentially. One of the names that has been given to this specific format is management information.

4.2 Module for managing UPnP devices

Users who are situated at a much larger distance are able to find ZigBee devices, and as a result of this, they are able to restrict access to ZigBee devices. This is a consequence of the fact that this is the case. The development of the UPnP service discovery protocol is a task that falls within the purview of the UPnP Forum, which is responsible for taking on this role. In order to facilitate communication between a wide variety of electronic devices that are connected to a local area network, this protocol was designed with the primary objective of facilitating such communication. The creation of this protocol was primarily aimed at accomplishing this particular goal.

5 Execution and analysis

In addition to doing mathematical analysis and verifying the design's actual performance, the suggested architecture is also built using open-source software. Using the proposed architecture, we carry out mathematical analysis and verify each function in the implementation environment. These functions include the template operation, fault detection and fault recovery functions, among others.

5.1 Implementation

In order to perform an analysis, the suggested architecture was put into action inside the setting shown in Table 1. We used four separate servers, each of which had a controller as well as three computer nodes. In order to ensure the controller's compatibility with the operations of cloud management, service drivers and monitoring drivers were installed. For the purposes of this essay, the monitoring server was situated inside the controller; however, it is feasible to configure it to function independently of the controller.

In this particular implementation, the procedure that must be undertaken in order to make availability accessible is shown in Figure 14. Following the construction of a Virtual Network Function (VNF) via the use of a Zabbix monitoring template, an Apache server was subsequently installed inside the designated VNF. Immediately after that, a straightforward application for the Internet of Things was deployed on the VNF. A fault detection and recovery method that has been registered in the service can be seen in Figure 15, and it is based on the information that was described in the template. This method is an example of a fault detection and recovery method.

Table 1 Implementation specifications

Entity	Condition	Version
Physical Server(4)	- Intel® Xeon® processor D-1520, Single-socket FCBGA1667; 4-core, 8 threads, 45 W - RAM: 16 GB/Disk space: 256 GB - Controller Node (1)/Compute Node (3)	
Cloud OS	OpenStack stable	Queens
VNF Manager	OpenStack Tacker	Master

Figure 12 Schematic of UPnP components (see online version for colours)

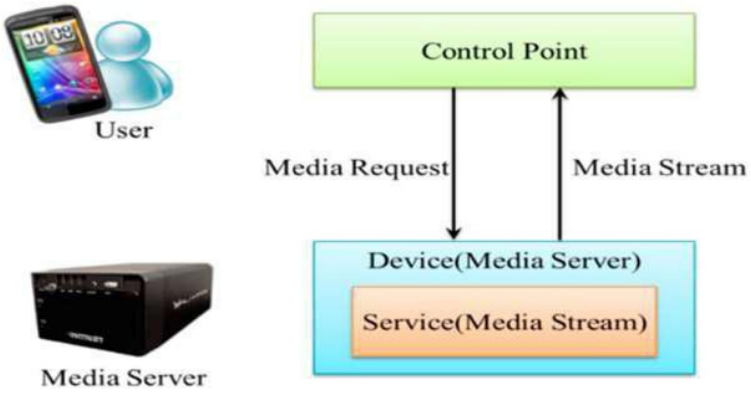


Figure 13 Descriptions of UPnP devices

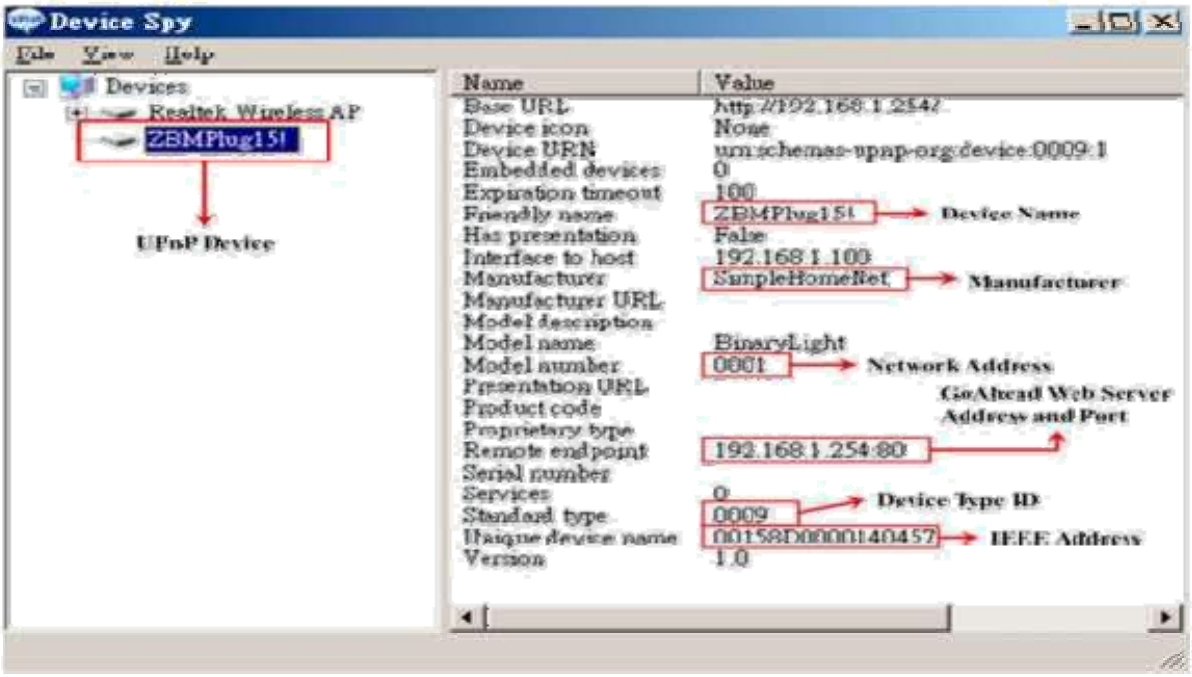


Figure 14 Procedure of service recovery for availability

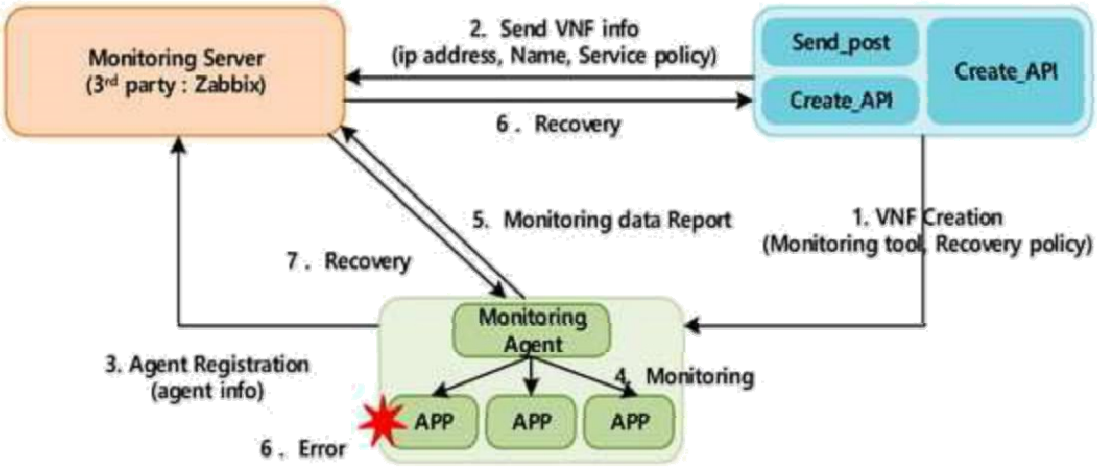


Figure 15 Example of VNF registration information (see online version for colours)

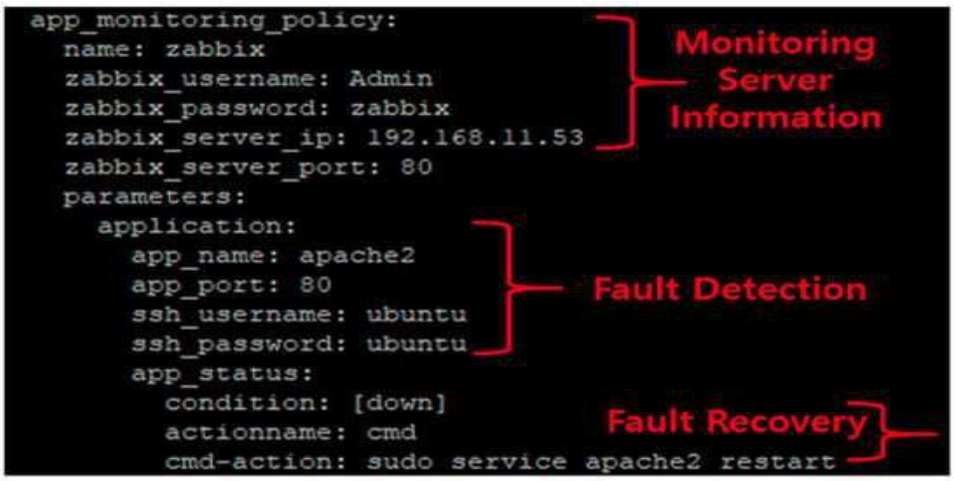
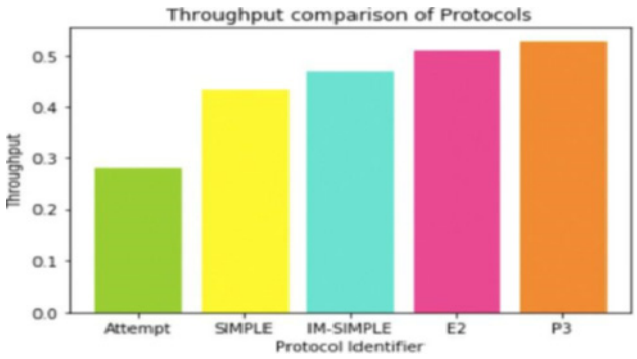


Figure 16 VNF registration on the monitoring server (see online version for colours)

6 Discussion

Following the completion of the study and testing, it was discovered that the proposed design provides a number of advantages that are not present in the existing architecture. These improvements may be observed in terms of the cost of deployment and the cost of monitoring resources, in addition to the performance of monitoring. The architecture that has been presented is organised in such a manner that it is capable of automatically setting fault detection and fault recovery mechanisms in line with the characteristics of Internet of Things services. The comparison bar chart is shown in Figure 17.

Figure 17 Internet protocols comparison (see online version for colours)



7 Conclusions

In order to solve the issue of the availability of a cloud environment for the Internet of Things (IoT), a new architectural framework was proposed. The practicability of the approach was shown by comparing it to the architecture that was already in place, and templates make it feasible to use the recommended method in accordance with the specifics of the delivery of the service. After being put to the test, the premise that the design provides the maximum possible availability for Internet of Things services was validated. The data were analysed, and it was discovered that the proposed system provides availability in a way that is both more dynamic and more efficient than the architecture that is already in place. This was discovered via the evaluation of the findings. In addition to this, the design that was recommended was implemented, and all of its capabilities were examined. During the course of future research, we want to do more research on the provisioning of availability in Internet of Things (IoT) cloud systems.

References

Centenaro, M., Vangelista, L., Zanella, A. and Zorzi, M. (2018) 'Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios', *IEEE Wireless Communications*, Vol. 23, pp.60–67. Available online at: https://build.sigfox.com/steps/certification/#what-is-a-sigfox-certification (accessed on 29 November 2018).

Cirani, S., Ferrari, G., Mancin, M. and Picone, M. (2018) 'Virtual replication of IoT hubs in the cloud: a flexible approach to smart object management', *Journal of Sensor and Actuator Networks*, Vol. 7, No. 2. Doi: 10.3390/jsan7020016.

Do, M.T., Goursaud, C. and Gorce, J.M. (2014) 'Interference modelling and analysis of random FDMA scheme in ultra narrowband networks', *Proceedings of the 10th Advanced International Conference on Telecommunications*, Paris, France, pp.132–137.

European Research Council (2018) *ERC Recommendation 70-03 relating to the use of short range devices*. Available online at: https://www.ecodocdb.dk/download/25c41779-cd6e/Rec7003.pdf (accessed on 29 November 2018).

Ferrández-Pastor, F.J., Mora, H., Jimeno-Morenilla, A. and Volckaert, B. (2018) 'Deployment of IoT edge and fog computing technologies to develop smart building services', *Sustainability*, Vol. 10. Doi: 10.3390/su10113832.

Fremantle, P. (2015) *A Reference Architecture for the Internet of Things*, White paper, WSO2, Colombo, Sri Lanka. Available online at: https://wso2.com/download/getfile/wso2_whitepaper_a-reference-architecture-for-the-internet-of-things.pdf (accessed on 29 November 2018).

Jamil, F., Iqbal, M.A., Amin, R. and Kim, D. (2019) 'Adaptive thermal-aware routing protocol for wireless body area network', *Electronics*, Vol. 8. Doi: 10.3390/electronics8010047.

Kharrazi, A., Qin, H. and Zhang, Y. (2016) 'Urban big data and sustainable development goals: challenges and opportunities', *Sustainability*, Vol. 8. Doi: 10.3390/su8121293.

Khutsoane, O., Isong, B. and Abu-Mahfouz, A.M. (2017) 'IoT devices and applications based on LoRa/LoRaWAN', *Proceedings of the IECON 2017 – 43rd Annual Conference of the IEEE Industrial Electronics Society*, Beijing, China, pp.6107–6112.

Lauridsen, M., Vejlgaard, B., Kovacs, I.Z., Nguyen, H. and Mogensen, P. (2017) 'Interference measurements in the European 868 MHz ISM band with focus on LoRa and SigFox', *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, San Francisco, CA, USA, pp.1–6.

Lee, S.K., Bae, M. and Kim, H. (2017) 'Future of IoT networks: a survey', *Applied Sciences*, Vol. 7. Doi: 10.3390/app7101072.

Mehmood, F., Ahmad, S. and Kim, D. (2019) 'Design and implementation of an interworking IoT platform and marketplace in cloud of things', *Sustainability*, Vol. 11. Doi: 10.3390/su11215952.

Mekki, K., Bajic, E., Chaxel, F. and Meyer, F. (2018) 'A comparative study of LPWAN technologies for large-scale IoT deployment', *ICT Express*, Vol. 5, No. 1, pp.1–7.

Montginoul, M. and Vestier, A. (2018) 'Smart metering: a water-saving solution? Consider communication strategies and user perceptions first: evidence from a French case study', *Environmental Modelling and Software*, Vol. 104, pp.188–198.

Park, E., Del Pobil, A.P. and Kwon, S.J. (2018) 'The role of internet of things (IoT) in smart cities: technology roadmap-oriented approaches', *Sustainability*, Vol. 10.

Raza, U., Kulkarni, P. and Sooriyabandara, M. (2017) 'Low power wide area networks: an overview', *IEEE Communications Surveys and Tutorials*, Vol. 19, pp.855–873.

Sigfox (2018) *M2M and IoT redefined through cost effective and energy ptimized*. Available online at: https://lafibre.info/images/3g/201302_sigfox_whitepaper.pdf (accessed on 29 November 2018).

SIGFOX Company (2018) *SIGFOX Company*. Available online: https://www.sigfox.com (accessed on 29 November 2018).

Voulvoulis, N., Arpon, K.D. and Giakoumis, T. (2017) 'The EU water framework directive: from great expectations to problems with implementation', *Science of the Total Environment*, Vol. 575, pp.358–366.

Wu, S.M., Chen, T.C., Wu, Y.J. and Lytras, M. (2018) 'Smart cities in Taiwan: a perspective on big data applications', *Sustainability*, Vol. 10. Doi: 10.3390/su10010106.