AN APPROACH FOR UTILIZING THE INTERNET OF THINGS FOR REMOTE MONITORING AND CONTROL SYSTEMS

Mihai Petre OPROIU[2*], Cristian Leonard MUȘUROI[1], Petru Adrian COTFAS[2], Daniel Tudor CORFAS[2], Marius VOLMER[1]

[1] *Department of Electrical Engineering and Applied Phyiscs Transilvania University of Brasov, Romania*
[2] *Department of Electronics and Computers Transilvania University of Brasov Brasov, Romania*

*Corresponding author: Mihai Petre OPROIU, mihai.oproiu@unitbv.ro

Abstract. *The development of IoT (Internet of Things) embedded solutions has grown exponentially in a wide range of applications. From simple solutions utilized by end users in the home automation sector to complex IoT implementations in the industrial sector, these applications have proven their usefulness and contribute to the proper functioning of the infrastructure in which they are operating. The slow migration from Industry 4.0 to Industry 5.0 opens new horizons, by implementing the aggregation, monitoring and control of data provided from Internet of Things (IoT) nodes. This work aims to serve as a general guide for utilizing a layered IoT architecture and for optimizing the design and workflow of IoT applications.*

Keywords: *cloud computing, control, edge computing, Internet of Things – IoT, Low Power Wireless Area Network - LPWAN*

Introduction

There are ever increasing requirements for diverse parameter monitoring in daily life. The development complexity of monitoring and control applications at a distance satisfies requirements from a simple parameter acquisition (e.g. ambient temperature detection), up to complex, production line monitoring and control and industrial robots. These technological advancements are due to significantly increased equipment processing power and also reduced costs of their acquisition. The technological advancement from the field of automation and communications has allowed the development of smart industry, otherwise known as Industry 4.0 [1]**.**

Industry 4.0 is an organization concept for smart devices and systems which at the basic level relies on: interconnecting elements of monitoring, action and control; information transparency through reliable data acquisition and processing; capacity for processing and manage decisions by implementing large scale AI (artificial intelligence) and EP (Edge Processing) and data security by implementing encryption and data protection mechanisms.

In the development of IoT (internet of things) integrated components (IoT node type), several challenges are present. One of the requirements of IoT nodes refers to the reduced size of the final hardware system. With miniaturization of IoT technologies, these can be integrated also in wearables (smart watches, smart telemedicine devices). Besides miniaturization, another important characteristic is the endurance of the system to environmental factors, both to natural meteorological conditions (e.g. humidity, high temperature fluctuations, dust, sunlight etc.) and industrial environments (e.g. electromagnetic radiation, optical radiation, vibrations etc.).

The information flow and bandwidth have to be adapted depending on the needs imposed by the application. These aspects are strictly connected to the type of protocols used for data transmission at a distance. In development of IoT applications, radio protocols from the LP-WAN (Low Power Wireless Area Network) are used: LoRaWAN, Sigfox, Zigbee, NB-IoT (Narrowband-IoT), LTE-M,5G, Wi-Sun, etc. [2-3].

Another essential aspect for choosing the protocol is the possibility for bidirectional communication between the final terminal and the system (uplink and downlink communication). This functionality allows control at a distance for software actualizations or maintenance for the equipment.

Also, the total energy usage of the IoT system is critical, even though the system can be supplied either through the grid directly (with adaptations) or using internal sources of the system. It is preferable that the device has energy independence for the system to function even when there are interruptions in the supply system. A good approach for energy efficiency in IoT systems is: maintain the device active only when it requires to collect or transmit data; limiting the number of messages transmitted through the network, the possibility to connect to a renewable energy source (photovoltaic panels with reduced dimensions, various energy harvesting systems) [4], and optimized designed through use of energy efficient transceivers and data transmission protocols. With these improvements, battery lifetimes that stretch to many years can be achieved [5].

Based on the aspects described above, the following work aims to serve as a general guide for IoT systems and implementing a layered IoT architecture based on the level at which data is processed.

Optimized layered IoT architecture depending on the level of data processing

For a better understanding of data distribution in IoT architecture, three level abstraction is used, Fig. 1.

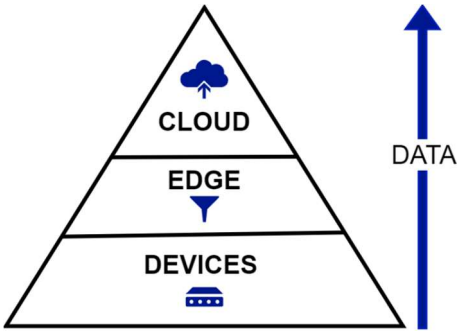

Figure 1. Layered IoT architecture on three levels (Device, Edge, Cloud) based on the level at which data processing occurs

The DEVICE layer, is the ensemble of hardware components necessary for data acquisition. In this layer, we can find the entire data acquisition and signal conditioning chain which allows measuring the variations of some physical quantities (electrical, mechanical etc.). This is achieved through various transducers and sensors located in the proximity of the device and connected to it.

From the data processing point of view, this layer is responsible for quality and quantity monitoring of raw data collected by the system. These aspects are directly correlated to the transducers and sensors capacity to satisfy the conditions imposed by the application (speed, resolution, stability, linearity etc.). In special conditions, in which the IoT equipment monitors variations of critical parameters, quality of the signal is paramount, even considering cost requirements.

The EDGE layer, is responsible with implementing methods and algorithms optimized for processing raw data from the device layer. On this layer, signal averaging or filtering processes can be implemented. Consequently, only relevant data will be transmitted at a distance, freeing bandwidth and slightly reducing energy usage.

The CLOUD layer has the purpose of storing and receiving data from the IoT nodes and terminals. Through the techniques promoted by the cloud computing technology, stability, scalability and redundance for applications by offering a generous and efficient environment for storing and processing data.

IoT applications

Nowadays, IoT applications are developing continuously and are used in various domains such as: smart cities, smart wearables, smart homes and smart vehicles, telemedicine, industrial internet of things (IIOT). A more detailed approach for the IoT architecture, offers the perspective of a five layered structure, Fig. 2. Depending on the implantation domain, different characteristics and technologies can be chosen for every layer.

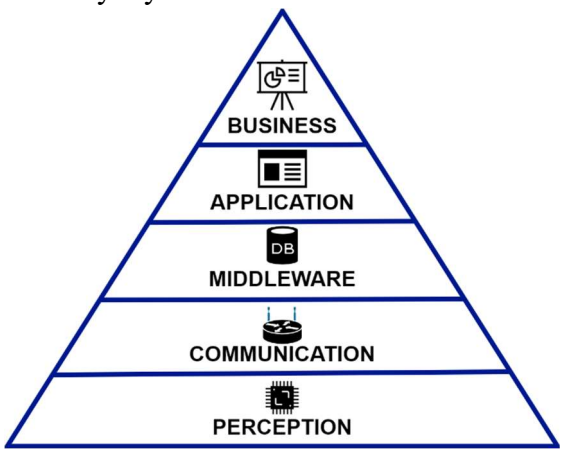

Figure 2. IoT architecture layerd on five levels
(Perception, Communication, Middleware, Application, Business)

In the PERCEPTION layer sensor types specific to the application are used. For example, for applications involved in the monitoring and control of air quality parameters in a smart city, we can choose sensors for temperature, humidity, atmospheric pressure, particles in suspension, volatile organic compounds, monitoring (e.g. DHT11, DHT22, BMP280, MQ135). For energy distribution applications (water, gas, heat), flowmeters can be used (e.g. YF-S201, YF-S401 or with higher endurance, depending on the application). For eHealth and telemedicine applications, biometric sensors are used for collecting various biosignals (pulse, oxygen saturation, electrocardiogram-EKG, electroencephalogram- EEG, feature detection) [6].

In the COMMUNICATION layer, depending on the application, the transceiver type and the utilized protocol, are selected. For applications with a low data rate and long-range transmission range, protocols such as LoRaWAN and Sigfox can be used. In the case of both long transmission range and high data rate (wide bandwidth), the NB-IoT or LTE-M protocols are recommended. For short range, usually Wi-fi, Zigbee or Bluetooth are implemented.

In the MIDDLEWARE layer, depending on the utilized protocol, gateway devices are selected for data acquisition from terminal devices. In case of smart devices networks, different topologies are used for each case, the most common being star topology.

In the APPLICATION layer, data is collected from the gateways distributed in the neighbouring zones of the IoT nodes. Within this layer, data from the end-chain devices can be collected.

The BUSINESS collection layer is used to gather collected data and can correlate data from multiple applications, subsequently being able to generate relevant reports. This final aspect improves the quality of the service and can allow for predictions for the behaviour of the system or parameters based on the generated reports.

Conclusions

Due to the continuous development of smart applications, the current and future requirements for parameter monitoring and data (gathering, processing, storage) needs are ever increasing for IoT applications. Careful considerations for the IoT architecture structure have to be taken and optimization for each link in the system architecture can be performed depending on the application,

whether referring to hardware or software components. In terms of hardware optimizations, it can be noted that application specific choices are mostly dependent on sensor performance, equipment endurance, reliability, versatility, energy usage and cost requirements. Each category for hardware optimization can have further enhancements, the most notable being the implementations of various power saving measures of supplementary power sources (renewable energy sources, energy harvesting systems). Regarding software optimizations, the choice of data transmission protocol and data processing chain are most essential for an efficient design, both in terms of energy usage and processing requirements, whilst still maintaining appropriate signal integrity.

The various hardware-software choices for the IoT application are necessary to be reflected throughout the entire structure of the IoT system and lead to major characteristics such as integrability, scalability, efficiency and reliability.

References

1. VAIDYA, S., AMBAD, P., BHOSLE, S. Industry 4.0–a glimpse. In: *Procedia manufacturing*, 2018, 20 , pp. 233-238. https://www.sciencedirect.com/science/article/pii/S2351978918300672?via%3Dihub
2. OPROIU, M., NEAGU, A., COTFAS, P., A., COTFAS, D., T., MUȘUROI, C., VOLMER, M. LoRa Wide-Area Network and Live Objects Used in Renewable Energy Monitoring. In: *2021 International Aegean Conference on Electrical Machines and Power Electronics (ACEMP) & 2021 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM)*, [Online], 2021, pp. 505-512 https://doi.org/10.1109/OPTIM-ACEMP50812.2021.9590023
3. MEKKI, K., BAJIC, E., CHAXEL, F., MEYER, F. Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT. In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Greece- Athens, 19 - 23 March, 2018, pp. 197-202 https://doi.org/10.1109/PERCOMW.2018.8480255
4. SHARMA, A., SHARMA, P. Energy Harvesting Technology for IoT Edge Applications. In: *Smart Manufacturing - When Artificial Intelligence Meets the Internet of Things.* London, United Kingdom: IntechOpen, 2021 [Online]. Available: https://www.intechopen.com/chapters/72195v https://doi.org/10.5772/intechopen.92565
5. PINTO, S., CABRAL, J., GOMES, T. We-care: An IoT-based health care system for elderly people. In: *2017 IEEE International Conference on Industrial Technology (ICIT)- 2017*, Canada-Toronto, 22 – 25 March, 2017, pp. 1378-1383 https://doi.org/10.1109/ICIT.2017.7915565.
6. YANG, W., WANG, S., SAHRI, N., M., KARIE, N., M., AHMED, M., VALLI, C. Biometrics for Internet-of-Things Security: A Review. In: *Sensors*, 2021, 21, 6163. https://doi.org/10.3390/s21186163