IoT Lysimeter System with Enhanced Data Security

Geraldo Oliveira, Carlos Almeida, João Miguel Santos, João C. Martins, and José Jasnau Caeiro(✉)

School of Technology and Management, Polytechnic Institute of Beja, Av. Pedro Soares, 7800-295 Beja, Portugal
{geraldo.oliveira,carlos.almeida,joao.santos, joao.martins,j.caeiro}@ipbeja.pt

Abstract. Diverse sources of data related to precision agriculture may be acquired with devices using an IoT architecture. Lysimeters are used to measure the amount of actual evapotranspiration released by plants, which is an important parameter for agriculture. New proposals of lysimeters extend the capabilities of these devices taking advantage of modern electronics, sensors, Internet, and computing devices. The paper presents an IoT based experimental lysimeter system implementation with enhanced data acquisition features. Some data is stored using a blockchain technology approach. The blocks are generated using an edge computing device. The special Linux operating system version for this device implements a trusted execution environment (OP-TEE). The paper describes the architecture of the system, the hardware implementation, and the data acquisition and blockchain software for the critical data generated by the smart lysimeter system, at the edge computing level.

Keywords: IoT lysimeter systems · Sensors · Data security · Blockchain · Trusted execution environments

1 Introduction

Modern agriculture uses data collected by sensors to improve water usage, increase production and enhance quality. It is commonly designated *precision agriculture*. One of the main purposes of the research work is to quantify the water requirement of plants in order to supply a more precise amount of water. Water is a fundamental good for the socio-economic development and agriculture consumes about 70% of freshwater, generally in an inefficient way. The lysimeter is an instrument that can be used on farms to allow reducing water consumption, on one hand, and to allow improving the productivity and quality of cultures, on the other hand. The quality and integrity of the collected data is essential to improve food production processes and their eventual audit. This naturally leads to the subject of modern blockchain technologies (BCT) and the

L. Brito Palma et al. (Eds.): CONTROLO 2022, LNEE 930, pp. 119–129, 2022.
https://doi.org/10.1007/978-3-031-10047-5_11

corresponding advantages in terms of data integrity. The quantification of the water requirement of plants is possible with lysimeters, which provide information on evapotranspiration. An IoT approach allows the design of enhanced low cost lysimeter systems.

Evapotranspiration (ET) is the amount of water that plants lose through evaporation and transpiration. In a crop there is a balance between water input and output. Rain, irrigation and condensation provide the water for the plant. However, the plant uses only the water which is released through transpiration, the remainder being lost through evaporation and drainage. Lysimeters are used to quantify the ET and allow the optimization of crop production by giving plants the exact amount of water they need for their healthy growth, obtaining huge water savings.

Decision support systems must allow a high degree of confidence on the data, to the users of the system. Data integrity must be ensured from the lowest data collection levels to the highest levels of data processing of the system. Lysimeter systems developed within the IoT framework [2], measure a number of additional parameters besides quantifying ET. They may include soil temperature and moisture at different levels, ambient temperature, humidity and light. IoT devices, due to their intrinsic low power characteristics, present new challenges for the security of the systems on which they operate.

Technological advances, combined with increasing creativity, have raised the levels of sophistication of attacks on information systems. While many security solutions rely solely on the quality of the software produced, it is becoming increasingly desirable to move from software engineering to hardware implementation of security in computer systems. Traditionally, much of the security in computer systems is cipher-based, consuming many resources in both processing and memory. These resources are reduced in IoT devices, making new mechanisms necessary to ensure security.

ARM, the leading producer of mobile processors and SoCs, has embraced security as a crucial factor in its system design. The ARM TrustZone technology enables the isolation of critical data or processes in a secure execution zone, isolated from the rest of the application and operating system, which is inherently insecure. The complexity of today's computing systems is extremely high, increasing the potential for vulnerabilities. Although the semiconductor industry applies a combination of different techniques to secure their embedded computing systems, the increasing sophistication of computer attacks use flaws that go beyond several layers of software and hardware and the latest exploits are an example of this. Security thus becomes an issue for the entire system, so that a combination of software quality and the implementation of security mechanisms in the hardware is the best option [4].

IoT systems capture large amounts of data from their sensors which are usually arranged in a distributed architecture that comprises computation and storage over a wide area network. Managing this information with security requires a combination of efforts with other technologies. In recent years, BCT has been proving its effectiveness and its distributed ledger-based architecture enables good integration into IoT systems [3,10].

Lysimeter data, when processed, can generate alerts and warnings for the farmer to take corrective action. Data manipulation can result in false alarms or warnings when everything is fine with the crop, or no alarms nor warnings when there is a problem, leading either to excessive water consumption or possible crop loss. To avoid this situations, the assurance that data is not altered neither manipulated throughout the chain, from collection to storage and processing, is very important. BCT can be used to ensure data integrity in these cases, one of the main goals of the system presented in this paper. This is mandatory in order to preserve the quality of the production chain. BCT allows a permanent, decentralized and integrated recording of data. It can be used for the identification of poor quality crops in the production chain, quickly and safely solving any eventual problem [9].

The paper describes a lysimeter system, developed in the IoT framework that measures other environmental and soil parameters in addition to evapotranspiration. These include: air temperature and humidity; visible luminosity; infrared luminosity; soil temperature and humidity at different depths. The system also captures images of the target crop for subsequent analysis for plant and pest control. A trusted execution environment and blockchain software is used to grant data security and integrity.

The document has the following structure. It starts with an introduction to the theme, a brief discussion on the subject, followed by a description of the work presented in this paper. In Sect. 2 a revision of the state of the art on IoT based lysimeter systems is made available to the reader. The implementation and the corresponding system architecture of the authors proposal is shown in Sect. 3. It presents the system parts, namely: the data acquisition; the edge computing and blockchain creation; and the data processing and transmission components. The paper concludes with a brief summary of the main achievements and some prospects for further development.

2 IoT Lysimeters

Some years ago, lysimeters were expensive devices used only by educational and research institutions. With the advent of the latest technologies, materials and sensors, it is now possible to build high-tech weighing lysimeters that are also more cost-effective. With an IoT approach, it is possible to build weighing lysimeters that can measure ET as well as other plant-related parameters, namely soil temperature and moisture, and environmental parameters, namely temperature, moisture and light. Weighing lysimeters usually have two vessels, one containing soil and plants and the other the drained water running off. The ratio of the weights of these vessels can be used to calculate ET.

Soils provide a range of ecosystem services that are beneficial for food production and environmental conservation. Healthy soil ecosystems are necessary to maintain supporting ecosystems, particularly the carbon and nitrogen cycles and water storage, preventing long-term soil degradation and increasing agricultural resilience to climate change. In [1] weighing lysimeters are used to study soil ecosystems. Lysimeters are used to analyse two different soil types (loamy sand, and silt loam) with different types of crops (soybean, winter wheat, corn, cover crop) and soil rotation techniques. Weighing lysimeters are used whenever an accurate ET estimate is required. Because of their better performance, they are also used to calibrate other devices, namely moisture sensors, or even other lysimeters, namely those without a weighing function. In [5] a weighing lysimeter is used to calibrate the *Diviner 2000* [8] capacitive soil moisture probe. This study allowed: the calibration of the probe for organic soils with a shallow water table; the verification of the calibration functions of the probe with the lysimeter; the verification of the difference between the calibration functions for organic soils and the standard calibration functions; the existence of a large difference between the water storage exchange of the lysimeter and the probe. In [6] it is described a small weighing lysimeter built to analyze the water infiltration in different types of soils. This lysimeter allows the study of the soil humidity and the water infiltration rate under steady rain conditions. The desert evapotranspiration is quantified in [11] using several humidity sensors at different depths associated with pressure sensors connected to a MCU, to monitor and maintain the soil humidity at a certain level. Its a non weighing lysimeter that needs also a calibration process. Another approach is followed in [7] where the ET is estimated recurring to a fuzzy neural network from temperature and atmospheric pressure data. After the training of the neural network the system is calibrated using a weighing lysimeter. All these lysimeters have no data security and integrity mechanisms.

3 An IoT Lysimeter with Enhanced Data Security

In addition to ET, the smart lysimeter presented in this paper, measures other parameters such as: soil temperature and moisture, at different depths; air temperature and humidity, and sunlight exposure (visible and infrared). The system also captures high resolution images of the crop which are sent to a remote server. This lysimeter monitors the crops in real time, making it possible to generate early warnings from the analysis of the collected data and make timely decisions related to crop control, pests and overall crop status. The trusted execution environment and blockchain software grant data security and integrity from the edge computing level to the data storage in the cloud.

The lysimeter system architecture consists of the following main parts: the lysimeter module; the edge computing module and the data analysis system, as shown in Fig. 1.

The *lysimeter module* sensors are connected to a low-power MCU that manages the data acquisition and transmission to the cloud through a radio-frequency telecommunication SoC module. The MCU also manages and monitors the power supply, turning on all circuits during data acquisition, processing and transmission, and turning them (sensors and SoC) off, to save power, according to the state machine in Fig. 2.

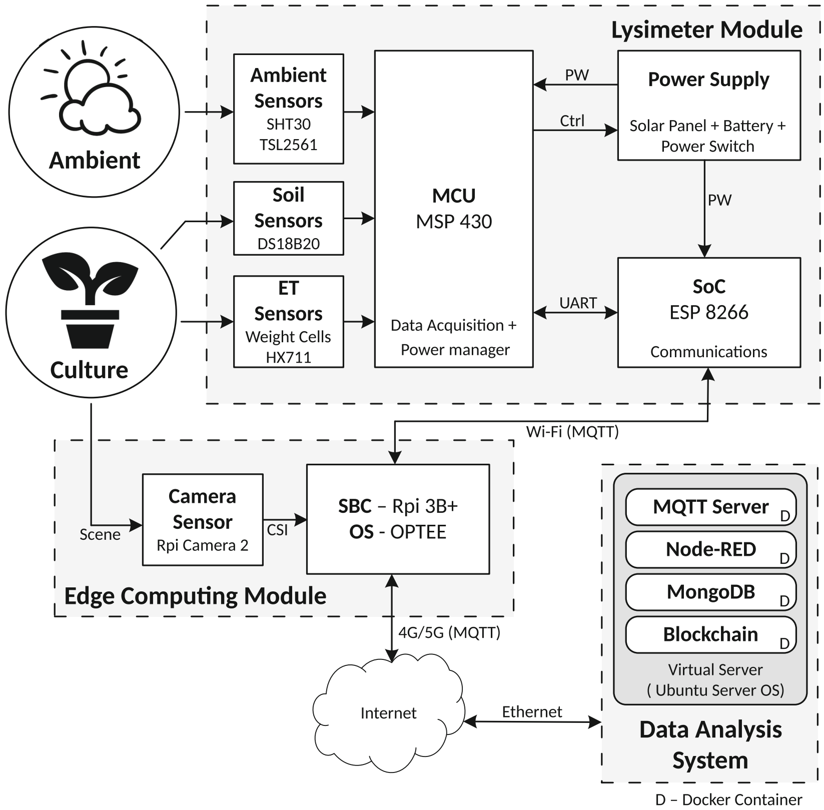

Fig. 1. The diagram references the sensors, processing devices, communication protocols and software stacks.

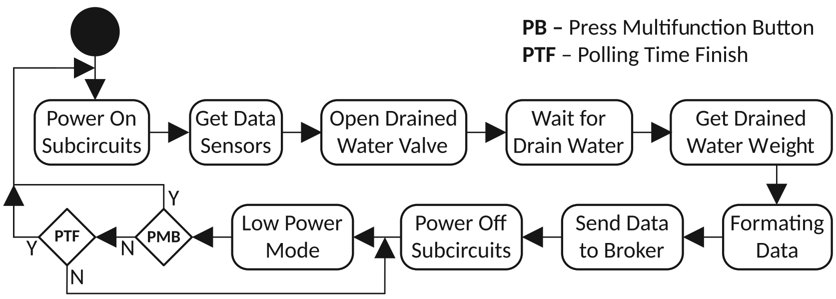

Fig. 2. Lysimeter module state machine: working principle with data acquisition, data transmission and power management.

The *lysimeter module* is built around the Texas Instruments MSP430G2553, an ultra-low power and low cost MCU with five power-saving modes. It has eight analog channels with 10-bit resolution and two digital 8-bit ports. The analog and digital ports are shared and can be programmed according to the inputs and outputs needed. The chip allows a maximum sampling rate of 200 kHz, far above the present needs of the system. Two I2C hardware channels allow for the connection of digital sensors, along with two SPI communication channels. The MCU also supports UART communication which is used to deliver the data to the ESP8266 device. The SoC was chosen because it has integrated WiFi support, compatible with IEEE 802.11b/g/n, thus reducing the design complexity and lowering the cost. This second MCU has a 32-bit ARM CPU architecture, running at 160 MHz. Besides other typical MCU characteristics, it has UART support. It must be emphasized that the proposed design has two MCUs because most of the time the MSP430 enters a low-power mode and controls the shutdown and wake-up of the energy circuitry thus effectively reducing the power consumption of the whole system. It only powers up the communication SoC when there is new data to be sent.

The evapotranspiration is formally obtained by $ET = k_m \Delta W/A$, where ΔW is the weight variation measured using the load cell amplifier HX711, with input from the weight cells using a Wheatstone bridge topology, A is the lysimeter floor area and k_m is a normalization and unit conversion constant. The ET dimensional units are mm per day, where one millimeter of ET is equal to the displacement of one liter of water into the atmosphere for every square meter of surface. The system takes into account the effect of sudden negative weight changes.

The HX711 is an analog to digital converter with a 24-bit resolution with integrated pre-amplification. The data is transmitted to the MSP430 using a proprietary synchronous protocol through two digital MCU IO ports. The soil temperature is acquired using sensors with *1Wire* communication protocol. These sensor measures the soil temperature with an accuracy of $\pm 0.5\,^{\circ}$C, in the $-10\,^{\circ}$C to $+85\,^{\circ}$C range. The *Grove* CMS - Capacitive Moisture Sensor was chosen for the estimation of soil moisture. It has an analog output that is connected to an analog port on the MCU. The moisture calibration is performed in the *internet cloud system*, as it can easily be adjusted according to the type of soil and crop. Soil moisture is estimated using capacitive sensors because they are more accurate and are resistant to corrosion than resistive sensors. The soil temperature and moisture are acquired at 3 different depths. The ambient luminosity, temperature and humidity are acquired with sensors using the I2C communication protocol. Namely, the SHT30 sensor, which measures the air temperature and humidity with an accuracy of $\pm 0.3\,^{\circ}$C, in the $-40\,^{\circ}$C to $+80\,^{\circ}$C range. This sensor also measures relative humidity in the 0 to 100% range with an accuracy of $\pm 2.0\%$. The luminosity is measured with the TSL2561 sensor, in the visible and infrared spectrum, with 16 bits resolution.

The *edge computing module* is supported by a Raspberry Pi 3B+ device. The OP-TEE trusted execution environment Linux operating system is used in this module. The OP-TEE (Open Source-Trusted Execution Environment) operating system is a special implementation generated with Buildroot, a tool designed for the creation of embedded Linux systems using cross-compilation. OP-TEE runs primarily on ARM based architecture devices and the main goal is to provide isolation from the non-secure operating system parts and the protection of *trusted applications* from each other using underlying hardware support. It comprises: a secure privileged layer; a set of secure user space libraries designed for usage by the trusted applications; a Linux user space library designed upon the TEE Client API, providing means to communicate with the trusted applications.

The term *trusted computing* is used to describe technologies that enable the implementation of security in local or remote computing systems. This is achieved by using components that guarantee the integrity of other parts of the system. Critical processes require additional protection from the operating system itself, which is inherently insecure. Therefore, it is necessary to ensure the isolation of the processes in a trusted execution environment (TEE) an area with processing capability, memory and data storage that is isolated from the system's main operating system. It ensures that data is stored, processed and protected in a secure environment. TEE provides developers with methods and tools to ensure that critical processes are isolated and sensitive data, encryption keys, authentication processes, *etc.*, are kept in storage zones that are protected from the operating system itself and from applications that may be corrupted. This method is intended to provide a complete separation of resources. Access to registers, caches, memory and peripherals is thus isolated from the potentially insecure native operating system. The code can execute with complete separation in the core, preventing access to any critical information of the process.

In the edge computing module the data is received and transmitted with a Mosquitto MQTT server special implementation. This is MQTTZ, a trusted zone server implementation that provides additional security. The edge computing module receives the data from the lysimeter module and creates a *block* based on a simple blockchain technology approach to secure data. Each block contains 4 elements: a timestamp; the sensorized data, part of a JSON data structure is represented in Table 1; a SHA512 hash value related to the last block in the blockchain and a generated SHA512 hash value from the timestamp, sensorized data and the previous block hash value. This effectively creates a great barrier to data tampering, thus allowing the system to be used in applications in the food supply industry, where the whole chain of production must be trusted. Periodically the locally produced blocks are transmitted to the data analysis system for further processing and storage.

The edge computing module is also used for the connection of a *Raspberry Pi* camera module that collects images from the surroundings of the lysimeter. These may be used for crop and pest detection or device security purposes. The 2nd version of the Raspberry Pi Camera Module, with 8 Mpx resolution, was chosen. It uses the IMX219 sensor from *Sony*, providing an excellent image quality in outdoor daylight conditions.

The lysimeter module has an average current consumption of 300 µA in low power mode (LPM) and 320 mA in operation mode (data acquisition and data sending). Considering a time interval of 10 min between readings and using a 3500 mAh and 3.6 V battery, the module works about 14 days using only battery power, without sunlight. The edge computing module consumes an average current of 300 µA in LPM and 1580 mA in operation mode (image acquisition, BCT data protection and data transmission), from a 3.6 V battery. Considering 3 moments of data transmission per day and a 3500 mAh battery, the module works around 20 days without sunlight. These features allow the system to operate continuously even in prolonged low-light conditions, for example in winter.

The *data analysis system* is built with an Ubuntu Server LTS virtual machine. Container technologies allow an easy deployment in a controlled environment of complex software stacks. The data analysis system adopts the Docker framework as the container software. The data analysis system also provides a Mosquitto MQTT server for data redistribution. The No-SQL MongoDB database management system retains a copy of the data because of the easy access provided to data processing applications. The blockchain is used to assure data integrity and backup storage. The Node-RED low code platform is used for easy data visualization.

A set of Internet services and ports, along with the data security component and clients, is represented in Fig. 3. The processed data is visualized in several types of devices: modern smartphones and tablets with a progressive web app (PWA) and traditional Internet browsers for data visualization and system management interface. Each edge computing module may receive data from several, not very distant, lysimeter modules.

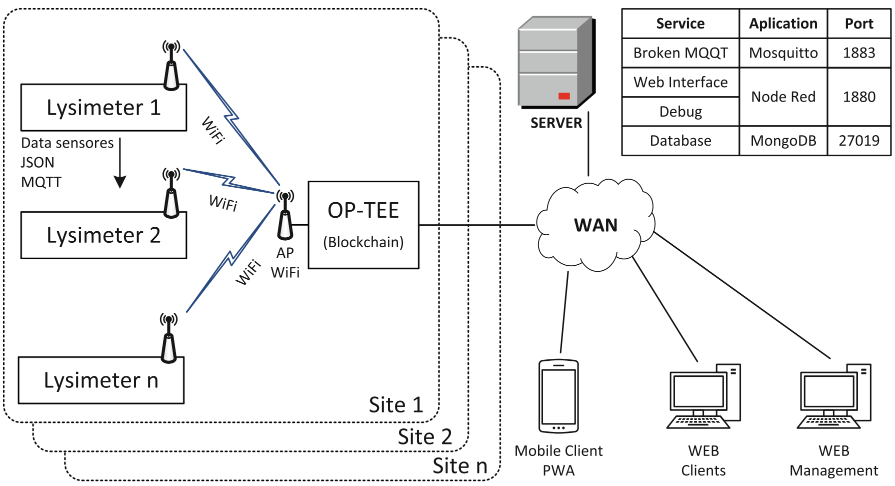

Fig. 3. Depiction of services and ports, the data security component and clients.

Table 1. Data description inside JSON.

Abr.	Description	Unit	Range/Accurancy
ID	Identification device	–	–
T	Timestamp	–	–
TA	Ambient temperature	°C	−40 °C:80 °C, ±0.3 °C
HA	Ambient humidity	%	0% : 100% RH, ±2%
L1	Visible + IR ambient luminosity	–	–
L2	IR ambient luminosity	–	–
TSx	Soil temperature	°C	−10 °C:85 °C, ±0.5 °C
HSx	Soil moisture	%	0% : 100% RH, ±10%
PL	Soil vessel weight	kg	0.00 kg : 50.00 kg, ±0.05 kg
PR	Drained water weight	kg	0.000 kg : 10.000 kg, ±0.005 kg
VB	Battery voltage	mV	–
NS	RF signal level	dBm	−105:−50 dBm

Fig. 4. Lysimeter and camera module prototype, and an example of a captured image.

The physical implementation of the lysimeter is presented in Fig. 4. In the left side there is the water collecting vessel filled with soil and an example of a plant (a strawberry bush). Attached to the vessel are the remaining devices. In the upper right corner there pictures of the solar panels and edge computing module with an attached Raspberry Pi Camera. The lower right side of the figure shows an image acquired with the camera device.

4 Conclusions

A modern IoT based lysimeter system is presented that measures: evapotranspiration; local ambient temperature, humidity and IR and visible spectrum luminosity; soil temperature and humidity at different depths. An additional feature is the imaging of the surrounding crop. The system is built using low cost sensors and processing elements, with very low power requirements (operating on battery and small solar photovoltaic panels). Low power mode consumes about 300 µA and the operating mode circa 320 mA. This roughly corresponds to 14 days only on battery support without solar incidence. The data is stored using a blockchain technology approach with blocks created in an edge computing device within a trusted execution environment operating system. These blocks are then afterwards incorporated into a main blockchain data structure. The information is transmitted to a remote data processing system using the MQTT Internet protocol and a resilient synchronous transmission for large sets of data. The users have access to the processed information with a PWA approach. The visualization is based on Node-RED. Although the system is only producing sensor data, it allows the design of applications for precision agriculture, namely: water usage; increased crop production and pest control.

Future development of the system may be focused on the introduction of improved edge computing devices, namely with advanced GPU processing, thus allowing machine learning capabilities *in-situ*. Further enhancements include long range wide area networking, e.g. LoRaWAN, thus allowing the deployment of this system over large areas and remote locations. The data processing and visualization system may also include artificial intelligence and the integration of the blockchain data with modern blockchain frameworks such as HyperLedger Fabric or IOTA. It is conceivable the integration into the system of remote detection data and local weather monitoring.

References

1. Brown, S., et al.: Assessing variability of soil water balance components measured at a new lysimeter facility dedicated to the study of soil ecosystem services. J. Hydrol. **603**, 127037 (2021)
2. Almeida, C., Santos, J.M., Martins, J.C., Caeiro, J.J.: Smart lysimeter with crop and environment monitoring: enhanced with pest and crop control. In: Camarinha-Matos, L.M., Heijenk, G., Katkoori, S., Strous, L. (eds.) IFIPIoT 2021. IFIPAICT, vol. 641, pp. 48–63. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-96466-5_4
3. Deepa, N., et al.: A survey on blockchain for big data: approaches, opportunities, and future directions. Future Gener. Comput. Syst. **131**, 209–226 (2022)
4. Dessouky, G., et al.: HardFails: insights into software-exploitable hardware bugs. In: 28th USENIX Security Symposium (USENIX Security 2019), pp. 213–230. USENIX Association, Santa Clara, August 2019