

Universidade de São Paulo (USP)

Faculdade de Filosofia, Ciências e Letras de Ribeirão Preto (FFCLRP)

Departamento de Computação e Matemática (DCM)

An IoT Smart Scale Proof of Concept for Smart Homes

Gabriel Carvalho Silva

Advisor: Cléver Ricardo Guareis de Farias

Ribeirão Preto – SP

2025

Abstract

This project proposal outlines the development of an Internet of Things (IoT) smart scale proof-of-concept (PoC) for smart home integration. The motivation for this work is to address key barriers to adoption in the field, specifically high costs, privacy concerns, and system scalability. This project aims to build a custom architectural solution to demonstrate a cost-conscious, privacy-by-design approach. The proposed system will consist of an embedded scale with facial recognition capabilities, a service layer for data management, and a client dashboard for data visualization and configuration. The design will emphasize an event-driven architecture using MQTT to ensure efficient and adaptive communication. Ultimately, this PoC will serve as a practical demonstration of best practices in the design of IoT systems, offering valuable insight into interoperability and performance trade-offs for smart home health devices.

Keywords: Internet of Things (IoT), Smart Homes, Embedded Systems, Facial Recognition, Adaptive Systems, Event-driven Architecture, MQTT, Proof-of-Concept

1. Introduction

The history of the Internet is a story of continuous expansion and integration. Starting in the late 1960s with ARPANET, a network for government and academic use, it was a tool for sharing information across an enclosed group of institutions and people. The adoption of the TCP/IP protocol in the early 1980s and the birth of the World Wide Web in the 1990s democratized this connectivity, paving the way to a modern digital world. Moreover, with the rise of affordable sensors, ubiquitous wireless technologies like Wi-Fi and 5G, and the vast processing power of cloud computing, the Internet's reach extended beyond traditional computers to encompass everyday objects. This transformation allowed devices to collect, share, and act on data autonomously, laying the groundwork for a “network of things”.

The Internet of Things (IoT) can be defined as “An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, react and act in situations faced and changes in the environment” [?]. IoT consists of an inter-network of physical devices like vehicles, buildings, and other items embedded with electronics, sensors, actuators, software, and network connectivity that allow these objects to collect and exchange data [?]. When these interconnected devices work within a household, they can be called a smart home system.

Internet-connected things include thermostats that can be controlled remotely from smartphones and smart body scales that allow one to graphically review the progress of diets using smartphones, for example. Moreover, smart scales detect gradual weight changes and, when integrated with smart home systems, create comprehensive health monitoring environments. This continuous data stream allows healthcare providers to intervene earlier and more precisely, potentially reducing hospital admissions and healthcare costs.

However, despite the increasing interest in IoT, the development of cost-effective IoT solutions currently face many different challenges. For instance, privacy features in many existing IoT development frameworks are relatively limited [?], which affects, for example, smart scale solutions reliability. Besides that, handling IoT sensor data, especially in terms of processing and integration with other data sources, has its own setbacks

[?]. Likewise, there is no ground truth for project design and architecture, which raises the question of which service composition mechanism best fulfills the functional scalability requirements of IoT systems [?]. On top of that, buying a scale can be financially challenging, particularly for low-income individuals, and scales with advanced features cost significantly more than scales without these features [?].

This project aims to deliver a working prototype of a smart scale with face recognition capability. Therefore, it consists of an embedded system for weighing a subject, a web service for managing weight records and performing face recognition, and a dashboard for data visualization. The development of the Proof-of-Concept (PoC) system takes into account cost and privacy concerns, as well as integration with legacy systems and scalability, considering many different possible architecture styles [?].

2. Related work

2.1. Smart Scale

The evolution of personal weighing devices from mechanical to electronic allow for better precision, ease of use and extra functionalities. The foundational technology of a modern electronic scale is a load cell, a transducer that converts mechanical force into an electrical signal. When an individual stands on the scale, a strain gauge undergoes a slight deformation. This deformation alters the electrical resistance of the gauge in a measurable way. An analog-to-digital converter processes this change, translating it into a precise digital weight value for display. While this technology significantly improved accuracy and usability over mechanical scales, its utility was confined to providing a single, instantaneous weight measurement.

The smart scale expands upon this foundation by integrating additional sensors and a communication module. These supplementary means provide a way to reshape the usage of a scale, or even add new functionality to it.

The connectivity of smart scales, typically through wireless protocols such as Bluetooth or Wi-Fi, is what defines their “smart” functionality. This capability facilitates the automatic and seamless transmission of collected data to a companion application or cloud-based service. This automated data flow eliminates the need for manual

record-keeping, thereby supporting long-term, continuous health tracking. The compiled data can be visualized and analyzed over time, which supports a shift from reactive to preventive healthcare.

However, the adoption of this technology faces challenges. Research by Mafong et al. [?] indicates that while there is a general willingness to use smart scales, affordability remains a significant barrier for many consumers. The study found that a notable portion of potential users were unwilling or unable to purchase such a device, highlighting the need for cost-conscious development.

2.2. Privacy in IoT systems

The explosive growth of the Internet of Things, particularly within the intimate setting of the smart home, has introduced a new and complex set of privacy and security challenges. Unlike traditional computing devices, IoT devices (also referred to as Smart Things) are often embedded into everyday objects, collecting vast amounts of granular, and often highly sensitive, personal data without the user's continuous, conscious interaction. This data can range from health metrics and daily routines to audio and video recordings captured by devices like smart speakers and cameras. The collection, transmission, and storage of this sensitive information create a vast surface area for potential security vulnerabilities and privacy breaches.

A central issue is the lack of privacy-by-design principles in many commercially available IoT devices and their corresponding development frameworks. This can lead to a host of security weaknesses, including weak authentication mechanisms, the transmission of unencrypted data, and an absence of user controls for managing personal information. The decentralized and heterogeneous nature of IoT ecosystems further complicates matters. A smart home can consist of devices from multiple manufacturers, each with its own security standards and data handling policies, making it difficult for a user to have a complete understanding and control over their data.

The use of biometric data, such as facial recognition in the context of the proposed Proof-of-Concept (PoC) smart scale, introduces a particularly acute privacy risk. If a biometric database is compromised, the user's identity is permanently at risk. This is a critical area that requires advanced security solutions. The work of Elordi et al. [?]

offers a compelling example of how to address this challenge. They propose a system that uses homomorphic encryption to protect this sort of data securely for elderly care applications. Homomorphic encryption allows computations to be performed on encrypted data without the need to decrypt it first. In the context of facial recognition, this means that the face matching process can occur on a server without the server ever having access to the unencrypted biometric template. This approach provides a powerful layer of privacy protection, as even if a database were to be breached, the data would remain encrypted. This PoC should build upon this by exploring secure data handling for facial recognition within a cost-conscious, smart home-oriented architecture, aiming to demonstrate how such advanced privacy measures can be integrated into a practical PoC.

2.3. Communication between IoT system devices

Naturally, communication is a key layer upon which any IoT solution is built and it involves a careful consideration of both the physical infrastructure and the logical architecture. At the physical layer, devices need to communicate wirelessly, and the choice of technology depends heavily on the specific application's requirements for bandwidth, range, and power consumption. For example, Wi-Fi is a common choice for many smart home devices due to its high bandwidth, which is essential for data-intensive tasks like streaming video from a security camera, and its widespread availability. However, Wi-Fi is also relatively power-intensive, which is a major drawback for battery-operated devices that need to run for months or years without a charge.

In contrast, Bluetooth, and its more energy-efficient variant, Bluetooth Low Energy [?], is optimized for low-power, short-range communication, making it an ideal choice for wearable devices, fitness trackers, and other battery-powered sensors. Still, other emerging technologies such as LoRa [?], which is specifically designed for long-range, low-power communication, are more suited for applications in smart cities or large-scale industrial IoT, as highlighted by Kane et al. [?].

This smart scale prototype should weight these options considering their range and bandwidth to handle both weight data and camera images, while acknowledging the power trade-offs.

Beyond the physical layer, the logical architecture of communication is crucial to

ensuring scalability, efficiency, and responsiveness in a heterogeneous IoT environment. The traditional request-response model, often implemented via HTTP/REST API calls, is a synchronous pattern in which a client sends a request to a server and waits for a response. This model is well-suited for many web applications but can be inefficient in an IoT context where devices may be intermittently connected and need to send data proactively rather than waiting for a request. A more robust and scalable solution for IoT is an event-driven architecture (EDA). In this paradigm, devices and services operate asynchronously, communicating through the publication and subscription of “events.” For example, when a user steps on the scale, the embedded system publishes a “weight-measured” event to a central message broker. Other services, such as a data processing worker or the face recognition service, that are interested in this event are automatically notified.

This publish-subscribe model, which is often facilitated by a lightweight messaging protocol such as Message Queuing Telemetry Transport [?], is highly advantageous for IoT systems. MQTT is designed for resource-constrained devices and low-bandwidth, high-latency networks, making it an ideal fit for the project. An EDA allows for loose coupling between components, meaning a new device or service can be added to the system without requiring changes to existing components. This modularity is a key factor for scalability and adaptability. In addition, it enables adaptive, context-aware data acquisition strategies.

In a system with low-frequency sensor data (weight) and high-latency operations (image processing for facial recognition), an event-driven model can optimize bandwidth and energy consumption. The system can be configured to only publish data when a significant change occurs (e.g., a weight measurement crosses a certain threshold) or when a specific condition is met, avoiding the need for continuous, wasteful polling. This adaptive approach is central to the proposed system’s design, aiming to improve responsiveness and reduce resource consumption in a real-world smart home environment.

3. Methodology

This project addresses the mentioned challenges by focusing on a PoC that balances advanced features with an economical design based on accessible hardware projects, such as the ESP32, thus contributing to the accessibility of smart home health monitoring solu-

tions. Furthermore, the PoC should also consider different architectural solutions, before choosing the most suitable one in order to guarantee extensibility, reliability, privacy and scalability.

In order to fulfill the project, the following activities are proposed:

1. Literature Review

This activity includes state-of-the-art review as well as related work study to build the theoretical foundation and argumentation of the final paper.

2. System Design and Implementation

Based on literature review and the knowledge acquired throughout the degree, this activity includes the design of the prototype system and its implementation. The system includes both hardware and software artifacts. Also, a Kanban [?] methodology is to be followed to guide the completion of the project.

3. System Metrics Definition and Implementation

Following the system implementation, this activity aims to define and implement a number of metrics to establish system performance within the defined objectives of the project.

4. System Evaluation and Documentation

This activity aims to evaluate the overall performance and functionality of the system.

5. Writing and presentation

Along with most steps of the project, the final paper is one of the main artifacts to be delivered by the conclusion of the project. Nevertheless, a presentation will be prepared to showcase the obtained results.

Table 1. Project Development Schedule

Task ID	Task Description	Aug	Sep	Oct	Nov	Dec
1	Literature review	x	x			
2	System design and implementation	x	x	x		
3	System metrics implementation		x	x	x	
4	System evaluation and documentation			x	x	
5	Writing and presentation			x	x	x

Table ?? presents the project development schedule.

4. Expected outcome

With the realization of the proposed project, new light is expected to be brought to the current state-of-the-art in IoT System Design for smart homes systems. Moreover, with the completion of this work, the expected deliverables include:

- A fully operational prototype for adaptive data acquisition and delivery.
- A dashboard to visualize and configure the system.
- Measurement of system response and message frequency.
- A discussion of system performance.