UNIVERSITY DE SÃO PAULO
FACULTY OF SCIENCES AND LETTERS OF RIBEIRÃO PRETO
DEPARTMENT OF COMPUTING AND MATHEMATICS

GABRIEL CARVALHO SILVA

An IoT Smart Scale Proof of Concept for Smart Homes

Ribeirão Preto–SP

2025

A minha avó, Maria Daria Rocha, e ao Gabriel de 10 anos que desenhava ideias e projetos em papel manteiga.

Acknowledgements

Agradeço . . .

Abstract

This final paper develops 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 developed system consists 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 emphasizes an event-driven architecture using MQTT (Message Queuing Telemetry Transport) to ensure efficient and adaptive communication. Ultimately, this PoC will serve as a practical demonstration of best practices in the design of IoT systems and of the application of novel approaches in edge computing, 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

List of figures

List of tables

List of abbreviations and acronyms

TODO   TODO

List of symbols

Γ   TODO

Summary

<div align="right">1</div>

Introduction

1.1 Background

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", or Internet of Things (IoT).

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, for example, for healthcare agents to intervene earlier and more precisely, potentially reducing hospital admissions and healthcare costs (PANJA et al., 2025).

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 (JIN; KUMAR; HONG, 2020a), 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 (SATHYAMOORTHY et al., 2024). Likewise, there is no ground truth for project design and architecture, which raises the question of which ser-

vice composition mechanism best fulfills the functional scalability requirements of IoT systems (ARELLANES; LAU, 2020). 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 (PARK et al., 2021).

1.2 Objective

Within this context, 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 and capturing their face image, a web service for managing weight records and performing face recognition, and a dashboard for measured data visualization.

The development of the Proof-of-Concept (PoC) system takes into account cost and privacy concerns, as well as system scalability, considering different possible architecture styles (MARTINO et al., 2018). It also explores and validates different aspects of such a system and their specific challenges following novel approaches from literature.

1.3 Methodology

This work followed the literature review to guide the understanding of current state of the art regarding IoT Systems, specially related to smart scales and privacy-aware scopes. Therefore, in order to follow up with the design and implementation of the system and subsequent evaluation of it, we opted for the ESP32 (the ESPCAM model specifically) as an accessible option for hardware solution and set a requirement for ESP32 compliant face embeddings extraction methods. Not only that, the architecture was defined by considering simplicity and extensibility capabilities besides functional requirements.

Several architectural styles were considered from current state of the art (MARTINO et al., 2018), leading to the adoption of a reactive event-driven architecture. This decision is aligned with the nature of the expected functionality of a smart scale, in which retry policies were implemented for when face recognition failed, and in which system components can be decoupled for extensibility.

Therefore, the ESP32 was calibrated for weight measurement and implemented the face embedding extraction using pre-trained models, an event queue was used to bridge system components, a web service was developed to manage data acquisition and retrieval and a dashboard was also created to visualize weight measurements.

Finally, the usage of the system as a whole was put under daily tests leading to conclusions regarding the actual feasability of the solutions for the challenges concerning

cost, privacy and performance.

1.4   Structure of this paper

The following chapters explore in more depth the various aspects of this project: Chapter 2 reviews literature and related work; Chapter 3 details the PoC development; and Chapter 4 brings to light the findings of this project.

Theoretical Foundation

2.1   Internet of Things

The Internet of Things (IoT) can be defined as an open and comprehensive network of intelligent objects that have the capacity to organize themselves, share information, react and act in situations faced and changes in the environment (MADAKAM, 2015). 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 (JAIN; TANWAR; MEHRA, 2019).

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 (MOCRII; CHEN; MUSILEK, 2018).

In contrast, Bluetooth, and its more energy-efficient variant, Bluetooth Low Energy (WOOLLEY, 2019), 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 (SORNIN et al., 2015), 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.* (KANE et al., 2022).

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 (MQTT) (STANDARD, 2019), 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.

2.2   IoT Sensors

IoT devices are also called Smart Things, which can also be perceived as physical objects connected to the web with some sensing capabilities (MADAKAM, 2015). Sensing is made possible by pairing embedded devices with sensors, actuators and other sorts of appendixes. Sensor are crucial for acquiring data and providing context for the interoperability of different IoT devices (PANJA et al., 2025).

Sensors can be of many kinds and for many purposes. Temperature, umidity and proximity sensors are some examples of it. Weight sensors specifically are commonly a

composiiton of load cells. The most widely used load cell is the strain gauge which is a thin foil resistor, the primary sensing element (MULLER et al.,). Strain gauges measure variations in voltage once they are deformed, because the intensity of the electrical resistance variation in the strain gauges is proportional to the intensity of the applied force that deform them (MULLER et al.,).

2.3   IoT System Architectural Styles

Figure 1 shows a simplification of an IoT architecture focused on cloud solutions. The cloud computing approach offers high processing power and storage option, while edge computing is more limited when it comes to computing power. However, edge computing achieves privacy measures more easily than the cloud. Nevertheless, fog computing is another approach that takes processing power closer to embedded devices on the edge, while still keeping the cloud layer unaware of sensitive information (MOCRII; CHEN; MUSILEK, 2018). Therefore, depending on the goals for a project, the placement of system components and tasks should be placed accordingly to what every computing layer offers and limits.

Figure 1 – Cloud-based architecture of a smart home. (Screenshot from (MOCRII; CHEN; MUSILEK, 2018, Fig. 1))
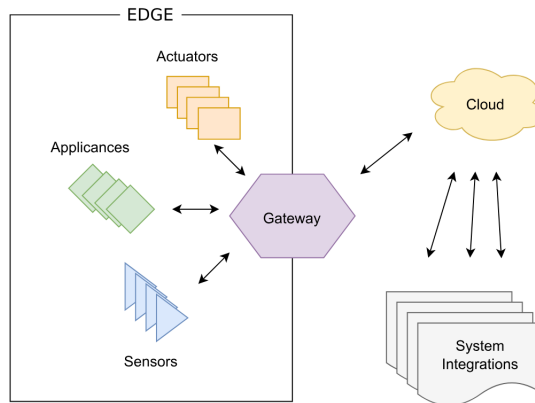
2.4   Smart Homes

A smart home system forms when interconnected devices, embedded with electronics, sensors, software, and network connectivity, work within a household. Mocrii *et al.* (MOCRII; CHEN; MUSILEK, 2018). define this system as having complementary user and system functions built upon a general IoT-based architecture. The devices themselves, often referred to as 'Smart Things,' possess embedded intelligence, identification, and automation capabilities designed to assist human life.

Seo *et al.* (SEO et al., 2015) proposed the Hexagonal Platform Architecture (HePA) as a reference architecture specifically designed for the complex, interconnected nature of the IoT era, including smart homes. Their implementation was a platform architecture model that aimed for extreme scalability while maintaining required performance. The article acknowledges the primary challenge as the advent of the complex IoT era, where all devices are interconnected, requiring enormous amounts of interaction. The article showcases a generic application, making extensive use of ports and adapters (hexagonal pattern) to integrate different data sources and data destinations, as well as third-party services, and by doing so, it presents solid foundation for a reference architecture pattern to be followed.

Jin *et al.* (JIN; KUMAR; HONG, 2020b) proposed the Peekaboo framework to provide architectural support for building privacy-sensitive smart home applications following homomorphic (a structure-preserving map between two algebraic structures of the same type) encryption of sensitive data. Their implementation philosophy moves pre-processing tasks (e.g., face detection) from the cloud onto a user-controlled hub. They achieved this by extracting image embeddings before sending data to the cloud. The authors primarily addressed the challenge of reducing data egress and minimizing potential privacy risks by preventing raw data from leaving the user's control.

Khazbak *et al.* (KHAZBAK et al., 2020) designed TargetFinder, a system that finds targets using crowdsourced IoT camera videos while preserving privacy. Their implementation achieved privacy preservation by exploiting homomorphic encryption techniques, which allows a system to search for the target using encrypted information. The system also includes techniques to ensure the requester receives only images containing the target, thereby protecting bystanders' images. The authors faced the major challenge of high computation overhead from the cryptographic primitives, which required them to develop optimization techniques to run the protocol efficiently on mobile devices.

2.5   Smart Scales

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.

The adoption of Smart Scales provide a number of benefits, such as easiest health tracking my health professionals and integration with other smart gadgets (PANJA et al., 2025). However, the adoption of this technology faces challenges. Research by Mafong *et al.* (MAFONG; KIM; FUJIOKA, 2020) 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.

Hasti *et al.* (HASTI; PERMATA; ARIBOWO, 2025) developed an IoT-based digital weighing scale prototype to address the growing health concern of obesity. Their implementation utilized load cell sensors, an HX711 amplifier, and an ESP8266 microcontroller for weight measurement. A companion Flutter-based application (MyWeightApp) connected to Firebase provided data storage, visualization, and real-time tracking of Body Mass Index (BMI) calculation. The primary implementation challenge involved ensuring hardware accuracy; however, the authors' testing demonstrated a low 0.78 percent error rate, well within the tolerance threshold.

Jaiteh *et al.* (JAITEH et al., 2019) designed a multipurpose smart tracking system that functions as both a weighing scale and a human tracking system using gait analysis. The implementation featured a sensing platform built with eight load cells and an amplifier, which fed analog signals to an Arduino microprocessor for data processing, analysis, and representation. The authors powered the system with either a 9V battery or solar energy, indicating a focus on power efficiency and standalone operation. Their implementation focused on calibrating the load cells and testing the sensing platform's precision and accuracy against various static weights and different individuals.

Zargham *et al.* (ZARGHAM et al., 2023) introduced an Intelligent IoT-based Scale to automate the sales process for fruits and vegetables in small-scale retail. The implementation used a load cell with an HX711 amplifier for accurate weighing and integrated advanced computer vision using fine-tuned YOLOv5n and YOLOv7 models for item detection and identification. A Python script handled the pricing logic, and the au-

thors developed a Graphical User Interface (GUI) for customer display and bill generation. The main implementation challenge was achieving high accuracy and efficacy in real-time processing. Still, their models achieved high mean Average Precision (mAP) scores (0.98 and 0.987) and high processing speeds.

2.6   Privacy in IoT and Face recognition

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.* (ELORDI et al., 2021) 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.

3

The Proof of Concept (PoC)

This PoC consists of an embedded system with integrated sensors capable of weighing and identifying a subject alongside complementary services for face recognition and data storage. It also offers a simple dashboard interface for managing subject registration (referred as profiles) and visualizing available weight measurements of them realized with the sensor mentioned.

This section unfolds the details of designing and implementing the whole system and presents the decision process for every step and piece of it.

The system consists of three layers: the edge, the fog, and the cloud or application layer. The edge layer consists of a scale, an HX711 signal amplifier and an ESP32. The scale itself consists of a Wheatstone bridge built with straing gauge load cells, connected using standard copper wires. The load cells are then connected to an HX711 signal amplifier that is then connected to the ESP32.

The ESP32 is callibrated using known weights and programmed to poll variations in voltage caused by deformation of the strain gauges when a weight is placed on top of them. The ESP32 module comes with a camera that captures image once a given weight threshold is beated.

The calibration is done through the polynomial regression of the acquired ADC (voltage) value and respective known weight values, resulting in a curve that is used to map ADC values to weight measurements.

[TODO add here image of the curve and table of the values]

Both image feature vector and weight value are sent to an MQTT broker, which serves as a queue service. For the purpose of this PoC, the broker was set up in a personal computer and executed under a **docker container** for abstraction, but it could be deployed to a RaspberryPi or even another ESP32 for its lightweight nature.

The fog layer consists of the MQTT broker which acts as the gateway between the

embedded system and its gathered data users (cloud layer services). Nevertheless, the cloud layer includes both a Hub Service for managing measurements in the database and a dashboard for visualizing available measurements by profile as shown in 2.

Figure 2 – Dashboard overview
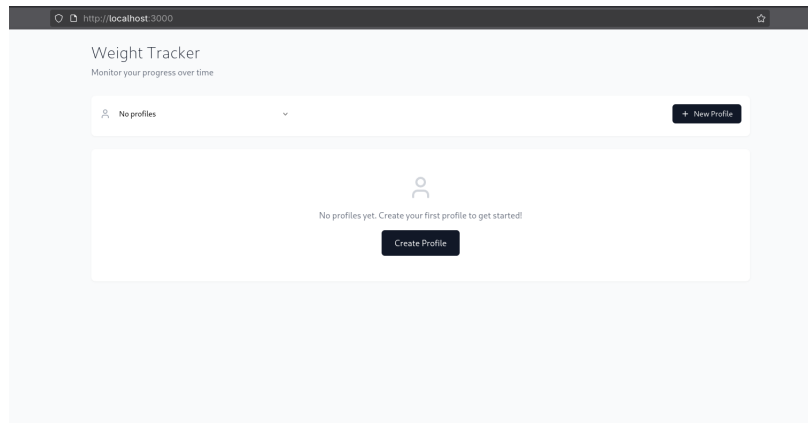
3.1 Project specification

3.1.1 Functional Requirements

The functional requirements (FRs) for the system define what it does from certain actor perspectices. The following functional requirements were identified:

1. The user shall be able to create profiles through a frontend client

    a) When creating a profile the user shall be able to name the profile

    b) When creating a profile the user shall be able to send a picture to be used for face recognition of the subject related to that profile

2. The user shall be able to access the available profiles and their available measurements

3. The user shall be able to measure their weight by stepping up on the scale when stepping up on the scale the system should then use its camera to match the subject.

3.1.2 Nonfunctional Requirements

Nonfunctional Requirements (NFRs) layout the qualities of a system, or *how* it should perform its functionalities. For this PoC, the following NFR were set:

1. The weight measurement must be accurate within an 100 grams margin of error;

2. The system shall account for measurement or face matching errors and support retry policies;

3. The system must be easily extensible to consider the possible adition of extra sensors and connection to outside systems;

4. Privacy is paramount and sensitive data such as biometric data shall never be saved in its raw format.

3.2   PoC Overview

In order to accomodate the FRs and NFRs, many engineering decisions were made based on literature review and good practices in software engineering and architecture. The embedded system is an ESPCAM (an ESP32 with built-in camera and SD card support) and its software was written in C, using Espressif libraries for MQTT and TensorFlow Lite pre-trained models for extracting face feature vectors from camera imaging. The MQTT broker is the Mosquitto by Eclipse implementation. Within the cloud layer, the data storage is implemented using PostgreSQL running pgvector plug-in for ease querying and storage of feature vectors. Still within the cloud layer, the Hub Service is implemented following the hexagonal architectural pattern and uses Kotlin with the Spring Boot framework for providing a web API and an MQTT client. Finally, we implemented a dashboard for easier visualization of the measurements. Figure 3 shows an overview of the whole solution. Notice in the figure **MobileApp** is not part of this PoC, but it exemplifies how the system could be easily extended. Other extensions to the system will be discussed in the Discussion section of the Conclusion chapter.

3.3   PoC edge layer

The **edge layer** contains the embedded solution with a weight sensor and a camera attatched to it. The solution was developed using an ESP32 microcontroller embedded with a 2 megapixel camera (ESPCAM), alongisde an HX711 signal amplifier chip. The weight sensor consists of a Wheatstone Bridge constructed with four strain gauges. Figure **??** shows how the Wheatstone bridge is created, the resulting system allows for measurement of up to 200Kg of weight. Figure **??** shows the actual load cell layout in the PoC.

TODO add image here for the conceptual wheatstone TODO take picture and add image here for actual load cell layout

Figure 3 – System overview and communication routes
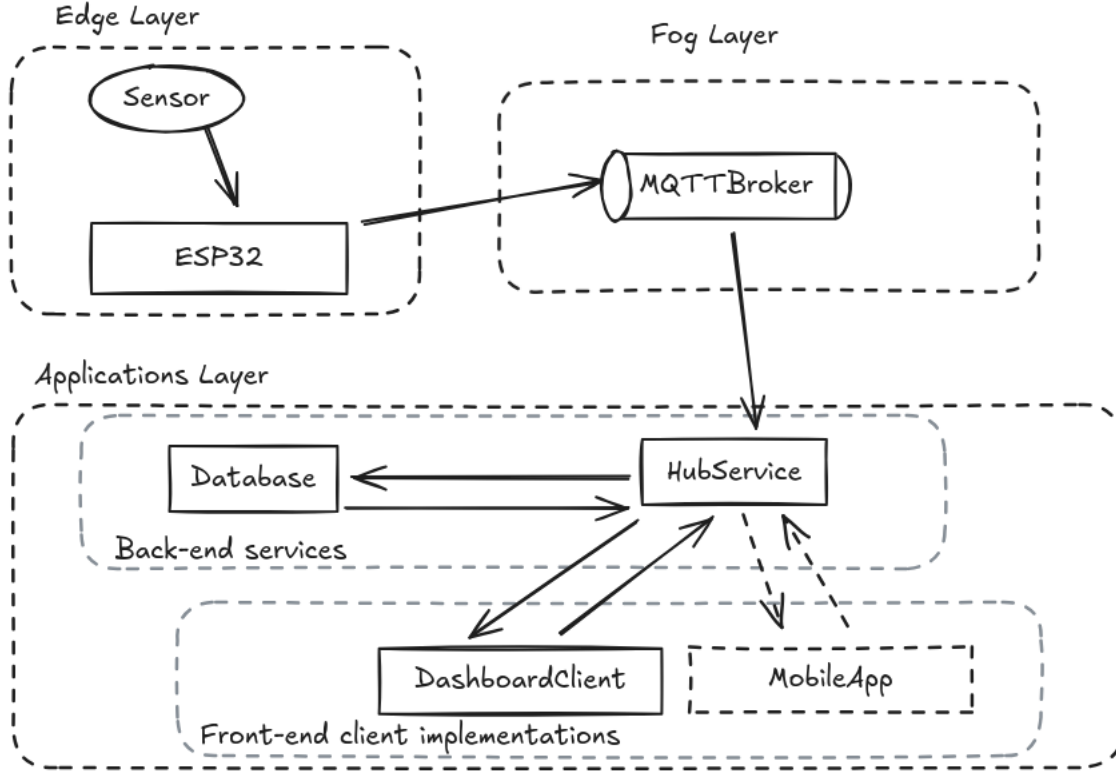
The ESP32 is aware of voltage variation to infer weight values based on callibrated reference values. Once a threshold is perceived, the camera is activated and an image is taken of the subject being weighed. Both weight and image information are sent to an MQTT broker that belongs to the next layer, the **fog layer**.

The callibration of the system was made through the measurement of voltage for known weight values by gradatively adding water to a bottle, measuring its weight with a kitchen scale and then measuring the difference in voltage perceived by the microcontroller. Those values are then fit to a curve through polynomial regression. The resulting sum of powers defines the function that maps ADC (Analog to Digital Converter) voltage read values to weight values.

TODO add table here with the values TODO add image here with the resulting graph

Once the weight beats a given threshold of 5 grams the scale is set to retire from its idle state and take a picture of the subject on it. The microcontroller makes use of the pre-trained MobileFaceNet model from TensorFlow Lite library to extract the feature vector from the image. By doing so, the subject image never leaves the (edge layer) and thus their privacy is protected by avoiding the transmission of possible sensitive biometric data to the **cloud layer**. Still, this feature vector is enough to query registered profiles in the database and follows the homomorphic encryption approach (JIN; KUMAR; HONG,

2020b).

TODO add image of the espcam face recon feature for representation of what happens

3.4 PoC fog layer

The **fog layer** consists of the intermediate services and tools for the system to work, however it still remains within the household domain. This means information here is still private to the local network (LAN). This layer can be deployed to a RaspberryPi, for example, to serve as an IoT Hub for smart things in the house.

For the sake of this PoC however, the RaspberryPi was replaced by docker containers run in a PC to represent it.

Within this project, this layer contains an **MQTT Broker**, a **face recognition service** and a **worker service**.

The MQTT broker serves as a queue service for bridging the edge layer to its required services. The **face recognition service** extracts a feature vector from the image (also referred as image embeddings) and queries for it in the database using an API, which belongs to the next layer, the **cloud or application layer**. Figure **??** shows this process.

Once the measurement is matched to a profile in the database, the **worker service** is able to upload it to the database through the same API used by the **face recognition service**. This is shown in Figure Figure **??**. If the image does not match any registed profile, then the ESP32 is notified through the inclusion of an error message in the MQTT broker as shown in **??**.

This workflow follows and Event-Driven Architecture (EDA) and is made possible through the definition of topics within the MQTT broker. The **??** shows the event flow for this subsystem of the PoC. Each event is always sent to its own topic, and services subscribe and publish to their topics of concern as shown in **??**.

3.5 PoC cloud layer

The **cloud layer** consists of a PostgreSQL database for storing profiles and their measurements, an API for managing those records and allowing for applications to rise and use the available data. For this PoC, an example application is set in the form of a dashboard, for managing profiles and visualizing the measured weights for them.

3.6 Smart Scale Face Recognition

The Face Recognition aspect of the system has its complexities of its own. Specially, the set privacy concerns required novel solutions. The images used for profile matching are never stored in order to keep privacy untouched.

The project uses an homomorphic encryption approach in which the feature vector of the system is used to represent it. This method allows for searching and comparison of images without the raw data.

This is made possible through the usage of the pgvector plugin within the PostgreSQL database used. It allows for storage and query of vector, which eases the process of matching profiles to weighing subjects.

Therefore, both during the registration of a profile and the taking of an image by the ESP32, the image embeddings are taken and used in place of the raw image data. This way biometric information is never stored, and is not kept in the **cloud layer**.

3.7 Project Evaluation

4

Conclusion

4.1   Contributions

4.2   Discussion

4.3   Future work

Applications to the Internet of Medical Things Applications to Husbandry

References

ARELLANES, D.; LAU, K.-K. Evaluating iot service composition mechanisms for the scalability of iot systems. *Future Generation Computer Systems*, v. 108, 03 2020.

ELORDI, U. et al. Optimal deployment of face recognition solutions in a heterogeneous iot platform for secure elderly care applications. *Procedia Computer Science*, v. 192, p. 3204–3213, 2021.

HASTI, L.; PERMATA, E.; ARIBOWO, D. Development of a Digital Body Weight Scale Prototype with IoT-Based BMI Calculation and Real-Time Weight Tracking. *Aviation Electronics, Information Technology, Telecommunications, Electricals, and Controls (AVITEC)*, v. 7, p. 31, fev. 2025.

JAIN, A.; TANWAR, P.; MEHRA, S. Home automation system using internet of things (iot). In: *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*. [S.l.: s.n.], 2019. p. 300–305.

JAITEH, S. et al. Smart Scale Tracking System Using Calibrated Load Cells. In: *2019 IEEE Conference on Sustainable Utilization and Development in Engineering and Technologies (CSUDET)*. [s.n.], 2019. p. 170–174. ISSN: 2473-3652. Disponível em: <https://ieeexplore.ieee.org/document/9214692>.

JIN, H.; KUMAR, S.; HONG, J. Providing architectural support for building privacy-sensitive smart home applications. In: *Adjunct Proceedings of the 2020 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2020 ACM International Symposium on Wearable Computers*. New York, NY, USA: Association for Computing Machinery, 2020. (UbiComp/ISWC '20 Adjunct), p. 212–217. ISBN 9781450380768. Disponível em: <https://doi.org/10.1145/3410530.3414328>.

JIN, H.; KUMAR, S.; HONG, J. Providing architectural support for building privacy-sensitive smart home applications. In: *Adjunct Proceedings of the 2020 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2020 ACM International Symposium on Wearable Computers*. New York, NY, USA: Association for Computing Machinery, 2020. (UbiComp/ISWC '20 Adjunct), p. 212–217. ISBN 978-1-4503-8076-8. Disponível em: <https://dl.acm.org/doi/10.1145/3410530.3414328>.

KANE, L. et al. Network architecture and authentication scheme for lora 2.4 ghz smart homes. *IEEE Access*, v. 10, p. 93212–93230, 2022.

KHAZBAK, Y. et al. TargetFinder: A Privacy Preserving System for Locating Targets through IoT Cameras. *ACM Trans. Internet Things*, v. 1, n. 3, p. 14:1–14:23, jun. 2020. Disponível em: <https://doi.org/10.1145/3375878>.

References

MADAKAM, S. Internet of things: Smart things. *International Journal of Future Computer and Communication*, v. 4, p. 250–253, 05 2015.

MAFONG, K.; KIM, S.; FUJIOKA, K. Are patients willing to use a smart scale? *Current Developments in Nutrition*, v. 4, p. 063–055, 2020. ISSN 2475-2991. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2475299123096750>.

MARTINO, B. D. et al. Internet of things reference architectures, security and interoperability: A survey. *Internet of Things*, v. 1–2, p. 99–112, 2018.

MOCRII, D.; CHEN, Y.; MUSILEK, P. Iot-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, v. 1-2, p. 81–98, 2018. ISSN 2542-6605. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2542660518300477>.

MULLER, I. et al. Load cells in force sensing analysis – theory and a novel application. v. 13, n. 1, p. 15–19. ISSN 1941-0123. Disponível em: <https://ieeexplore.ieee.org/document/5399212>.

PANJA, S. et al. 1 - internet of medical things: architecture, trends, and challenges. In: NGUYEN, T. A. (Ed.). *Blockchain and Digital Twin for Smart Healthcare.* Elsevier, 2025. p. 1–17. ISBN 978-0-443-30300-5. Disponível em: <https://www.sciencedirect.com/science/article/pii/B9780443303005000026>.

PARK, J. S. et al. Affordability and features of home scales for self-weighing. *Clinical obesity*, v. 11, p. e12475, 06 2021.

SATHYAMOORTHY, S. et al. Advances and challenges in IoT sensors data handling and processing in environmental monitoring networks. *HAFED POLY Journal of Science, Management and Technology*, v. 5, p. 40–60, 05 2024.

SEO, S. et al. HePA: Hexagonal Platform Architecture for Smart Home Things. In: *2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS).* [s.n.], 2015. p. 181–189. ISSN: 1521-9097. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7384294>.

SORNIN, N. et al. Lorawan specification. *LoRa alliance*, v. 1, p. 16, 2015.

STANDARD, O. Mqtt version 5.0. *Retrieved June*, v. 22, n. 2020, p. 1435, 2019.

WOOLLEY, M. Bluetooth core specification v5. 1. *Bluetooth Special Interest Group*, 2019.

ZARGHAM, A. et al. Revolutionizing Small-Scale Retail: Introducing an Intelligent IoT-based Scale for Efficient Fruits and Vegetables Shops. *Applied Sciences*, v. 13, n. 14, p. 8092, jan. 2023. ISSN 2076-3417. Publisher: Multidisciplinary Digital Publishing Institute. Disponível em: <https://www.mdpi.com/2076-3417/13/14/8092>.