Article

Not peer-reviewed version

PlugID: A Platform for Authenticated Energy Consumption to Enhance Accountability and Efficiency in Smart Buildings

Raphael Machado *, Leonardo Pinheiro , Victor Santos , Bruno Salgado

Posted Date: 23 July 2025

doi: 10.20944/preprints202507.1952.v1

Keywords: authenticated energy consumption; smart plug; energy efficiency; Internet of Things; user accountability; RFID authentication; smart buildings; energy monitoring; MQTT over TLS; behavioral energy management

 doi:10.20944/preprints202507.1952.v1

Article

PlugID: A Platform for Authenticated Energy Consumption to Enhance Accountability and Efficiency in Smart Buildings

Raphael Machado [1,*], Leonardo Pinheiro [1], Victor Santos [2] and Bruno Salgado [2]

[1] Clavis Segurança da Informação

[2] Green Hat Segurança da Informação

* Correspondence: raphael.machado@clavis.com.br

Abstract

Energy efficiency in shared environments, such as offices and laboratories, is hindered by a lack of individual accountability. Traditional smart metering provides aggregated data but fails to attribute consumption to specific users, limiting the effectiveness of behavioral change initiatives. This paper introduces the "authenticated energy consumption" paradigm, an innovative approach that directly links energy use to an identified user. We present PlugID, a low-cost, open-protocol IoT platform designed and built to implement this paradigm. The PlugID platform comprises a custom smart plug with RFID-based authentication and a secure, cloud-based data analytics backend. The device utilizes an ESP8266 microcontroller, Tasmota firmware, and the MQTT protocol over TLS for secure communication. Seven PlugID units were deployed in a small office environment to demonstrate the system's feasibility. The main contribution of this work is the design, implementation, and validation of a complete, end-to-end system for authenticated energy monitoring. We argue that by making energy consumption an auditable and attributable event, the PlugID platform provides a powerful new tool to enforce energy policies, foster user awareness, and promote genuine efficiency.

Keywords: authenticated energy consumption; smart plug; energy efficiency; internet of things; user accountability; RFID authentication; smart buildings; energy monitoring; MQTT over TLS; behavioral energy management

1. Introduction

The pursuit of energy efficiency has become a global imperative, driven by the need to mitigate climate change and optimize resource use. Buildings, in particular, represent a substantial portion of global energy consumption [1], accounting for over 40% of the world's energy use and greenhouse gas emissions. This fact positions them as a priority target for interventions aimed at sustainability.

Despite significant advances in building automation technologies, such as smart HVAC (heating, ventilation, and air conditioning) and lighting systems [1], a critical gap persists, especially in shared-use environments like offices, laboratories, and co-working spaces. In these locations, energy consumption is typically aggregated and anonymized, leading to a phenomenon analogous to the "tragedy of the commons", where individual responsibility is diluted. Without the ability to attribute consumption to specific users, initiatives to promote behavioral change and energy conservation lose much of their effectiveness.

To address this gap, this work proposes a new paradigm: **authenticated energy consumption**. This approach treats access to energy not as an invisible and unrestricted service, but as a controllable and auditable event, analogous to logging into a computer system. By requiring a user to authenticate to consume energy, we create a direct link between consumption and the responsible individual. This

 doi:10.20944/preprints202507.1952.v1

fundamental shift transforms energy management from a purely technological system to a socio-technical one that actively engages the user in the conservation process.

The materialization of this concept is the **PlugID** platform, an end-to-end solution developed as the main outcome of the "Smart Energy" research project. PlugID consists of a low-cost smart plug, equipped with an RFID reader for token-based authentication, and communicates through an open and secure data pipeline. The development of a proprietary solution was a strategic decision, motivated by the finding, during the project's survey phase, that most commercial meters available on the market operate on closed and proprietary platforms, preventing interoperability and the analysis of raw data. The PlugID platform, in contrast, was built on open-source firmware (Tasmota) and standard communication protocols (MQTT), offering an open and auditable alternative.

This article presents the complete architecture of the PlugID platform, details its hardware and firmware implementation, describes its deployment in a real-world test scenario, and discusses the security, privacy, and behavioral implications of the authenticated consumption model. The structure of the article is as follows: Section 2 reviews the state of the art in smart energy management, contextualizing our contribution. Section 3 describes the architecture of the PlugID platform in detail. Section 4 presents the demonstration scenario and deployment results. Section 5 offers a critical discussion on the impact, limitations, and future directions of the work. Finally, Section 6 presents the conclusions.

2. The State of the Art in Smart Energy Management

To contextualize the contribution of the PlugID platform, it is essential to analyze the current landscape of energy management technologies. This section reviews the monitoring paradigms, platform architectures, access control models, and security challenges that define the field.

2.1. Energy Monitoring Paradigms: ILM vs. NILM

Appliance-level energy consumption monitoring, known as Load Disaggregation, is fundamental to energy efficiency. Two main approaches dominate this field: Intrusive Load Monitoring (ILM) and Non-Intrusive Load Monitoring (NILM) [2].

Intrusive Load Monitoring (ILM) involves installing smart meters or sensors on each individual appliance or outlet. This approach is characterized by its high accuracy, as it directly measures the consumption of each load [2]. However, its disadvantages are significant: the cost of acquiring and installing multiple sensors can be prohibitive, the installation is complex, and maintaining a distributed sensor network is burdensome [2].

In contrast, **Non-Intrusive Load Monitoring (NILM)** seeks to overcome these barriers. Using machine learning and signal processing algorithms, NILM analyzes aggregated data from a single central meter (like a building's main meter) to disaggregate the consumption of individual appliances [3,4]. The advantages of NILM are the drastically lower installation cost and greater privacy preservation, as it does not require installing devices within the private space [3,4]. However, its main drawback is lower accuracy compared to ILM, especially in environments with many appliances or devices with multiple operating states [3,4].

The PlugID platform fundamentally fits into the ILM paradigm, leveraging its high accuracy. However, it advances the traditional ILM concept by introducing an additional and crucial layer of granularity: **user authentication**. While conventional ILM answers the question "What is consuming energy?", PlugID answers "Who is responsible for this consumption?". This extension transforms the meter from a simple monitoring device into a management and accountability tool. Table 1 provides a comparative analysis of these approaches.

 doi:10.20944/preprints202507.1952.v1

Table 1. PlugID, ILM, and NILM comparison.

Feature	Intrusive Load Monitoring (ILM)	Non-Intrusive Load Monitoring (NILM)	PlugID (Authenticated ILM)
Accuracy	High	Variable (lower than ILM)	High
Installation Cost	High	Low	Moderate (per measurement point)
Installation Complexity	High	Low	Moderate (plug-and-play)
Maintenance	Difficult	Easy	Easy (per device)
Privacy	Invasive	Preserved	Requires data governance policies
Granularity (Appliance Level)	Yes	Yes (inferred)	Yes
Granularity (User Level)	No	No	Yes (main feature)

2.2. IoT Platforms for Energy Management

IoT platforms that support energy management are typically structured in a multi-layer architecture, with the four-layer model being the most common: Sensing, Network, Data Processing, and Application [6,7].

1. **Sensing Layer:** Composed of sensors (temperature, humidity, occupancy) and actuators (relays, switches), this layer is the direct interface with the physical world, collecting data and executing commands.
2. **Network Layer:** Includes gateways and data acquisition systems that aggregate information from sensors, convert formats, and provide connectivity to broader networks, such as the internet.
3. **Data Processing Layer:** Acts as the central processing unit, where data is analyzed, pre-processed, and stored. Edge computing plays a growing role in this layer to improve efficiency.
4. **Application Layer:** This is the interface with the end-user, providing visualization dashboards, alerts, and control through cloud or local applications.

Communication within these platforms relies on a variety of protocols, such as Wi-Fi, Zigbee, Z-Wave, and MQTT, each with different trade-offs in terms of range, data rate, cost, and power consumption. One of the most persistent and significant challenges in the IoT ecosystem is the **lack of interoperability** [6]. The proliferation of proprietary standards and the absence of a shared infrastructure create "data silos," where devices from different manufacturers cannot communicate, hindering system integration and limiting the potential of smart energy solutions. This market reality validates the PlugID project's approach of building a solution based on open protocols and open-source firmware, ensuring interoperability and avoiding vendor lock-in.

2.3. Access Control for IoT Resources

In an IoT environment, electrical energy can be conceptualized as a finite and controllable resource, whose access can and should be managed. The application of access control models, traditionally used in information security, is therefore directly relevant. Recent literature on IoT security evaluates several models and their applicability [8–11].

 doi:10.20944/preprints202507.1952.v1

- **Discretionary Access Control (DAC):** In this model, the owner of a resource defines access permissions. Its static nature and the need for manual management of access control lists (ACLs) make it unsuitable for dynamic and large-scale IoT environments.
- **Role-Based Access Control (RBAC):** RBAC grants permissions based on roles assigned to users. While it simplifies administration in some contexts, it faces the problem of "role explosion" in heterogeneous IoT ecosystems and has difficulty supporting the necessary dynamism.
- **Attribute-Based Access Control (ABAC):** ABAC is widely considered the most promising model for IoT.[12] It makes access decisions based on policies that evaluate a combination of attributes of the subject (user/device), object (resource), action, and environment (location, time of day). This flexibility allows for the creation of rich, dynamic, and context-sensitive access policies.

The PlugID authentication mechanism represents a fundamental step towards implementing a complete ABAC system for energy management. The unique identifier (UID) obtained from the RFID token is a user attribute. In future work, this can be combined with other attributes—such as the type of connected device, the time of day, or user-specific energy quotas—to create highly granular and dynamic energy access policies.

2.4. Security and Privacy in Smart Metering Systems

The increasing connectivity of smart metering systems introduces significant security and privacy vulnerabilities. The most prominent security threats include data integrity attacks, such as false data injection (FDI), which can manipulate consumption readings; unauthorized access for information theft or device control; replay and man-in-the-middle attacks to intercept or alter communications; and Denial of Service (DoS) attacks to disrupt system availability [12].

Privacy risks are equally severe. High-granularity energy consumption data can be analyzed to infer highly sensitive information about a building's occupants, such as daily routines, presence and absence schedules, and even the types of appliances in use, creating a detailed profile of user behavior [13–16].

Mitigation strategies recommended by the research community focus on a defense-in-depth approach, including robust authentication mechanisms to verify the identity of users and devices, end-to-end encryption to ensure the confidentiality and integrity of data in transit, the use of secure communication protocols, anomaly detection systems to identify suspicious behavior, and strict access control policies. This security framework serves as the basis for evaluating the design of the PlugID platform, which will be discussed in Section 5.2.

3. The PlugID Platform for Authenticated Energy Consumption

The PlugID platform was designed as an end-to-end solution to implement the authenticated energy consumption paradigm. Its architecture integrates edge devices, a secure communication channel, and a cloud analytics platform.

3.1. System Architecture

The overall architecture of the PlugID system is composed of three main components, which ensure a secure and efficient data flow from the point of consumption to the analytics platform:

1. **The Edge (PlugID Devices):** At the level closest to the user, multiple PlugID devices are deployed in electrical outlets. The design includes different models (PlugID-E, PlugID-E/AT, PlugID-ETH) to meet various use cases, from simple monitoring to authenticated measurement and correlation with environmental data.
2. **The Communication Layer:** The devices at the edge use their Wi-Fi capabilities to securely transmit the collected data to a central broker. Communication is based on the MQTT (Message Queuing Telemetry Transport) protocol, which operates on a publish/subscribe model.

 doi:10.20944/preprints202507.1952.v1

3. **The Cloud (SmartEnergy Platform):** A central server hosts the MQTT broker (mosquitto) and the data analytics platform, named SmartEnergy. This platform is responsible for receiving, storing, processing, and visualizing the data. It was implemented using the Elastic Stack technology, with Elasticsearch for storage and indexing, and Kibana for creating visualization and analysis dashboards.

In this architecture, the PlugID devices act as "publishers," sending JSON messages to specific topics on the MQTT broker. The SmartEnergy platform acts as a "subscriber," subscribing to these topics to receive the data in real-time, which is then persisted for historical analysis and visualization.

3.2. The PlugID Device: Hardware and Firmware

The heart of the platform is the PlugID device, a custom smart plug whose hardware components were carefully selected to balance cost, functionality, and openness. Table 2 details the main components and the rationale for their selection.

Table 2. Hardware and firmware of PlugID.

Component	Model	Key Specifications	Rationale for Selection
Microcontroller	ESP8266 NodeMCU v2 - ESP12	Integrated Wi-Fi, 11 GPIO pins, analog-to-digital converter	Low cost, wide availability, active development community, sufficient processing power for the application.
Energy Measurement Module	PZEM-004T	AC voltage measurement, current (up to 100 A), power. Serial communication.	Indirect measurement via current coil (non-invasive), ease of integration, and simple data interface.
Authentication Module	MFRC522 RFID Reader	13.56 MHz frequency, supports MIFARE cards, SPI interface.	Market standard for token-based authentication, low cost, and mature software libraries.
Power Supply	Mini Hi-link 5V Power Supply	Bivolt input (100-240 VAC), 5 VDC output.	Compact and sealed, allows powering the circuit directly from the electrical outlet safely.
Environmental Sensor (ETH Model)	AM2302/DHT22	Temperature and humidity measurement.	Allows correlation between energy consumption and environmental conditions, aiding in deeper efficiency analyses.

The device's firmware is based on **Tasmota**, an open-source firmware for ESP8266-based devices. The choice of Tasmota was strategic due to its maturity, excellent support for MQTT and OTA (Over-the-Air) protocols, and, crucially, its powerful Rules Engine. This rules engine allows complex, stateful logic to be executed directly on the device (at the edge), making the system more resilient and less dependent on continuous cloud connectivity.

The user session management logic was implemented through two sets of rules:

- **Rule1:** This set of rules handles periodic and initialization events. One rule is triggered on system startup to obtain and store the device's MAC address, which serves as a unique identifier. Another rule is triggered periodically (every teleperiod) to publish a status message via MQTT, containing the MAC, an authentication capability indicator (TokenAuth), and the UID of the currently logged-in user (if any).
- **Rule2:** This set is dedicated to the RFID authentication logic. It is triggered by read events from the RC522 module. When a card is brought near, the rule checks if a session is already active. If not, it stores the card's UID, starts a new session, and triggers an LED for visual feedback. If a session is already active, the rule checks if the presented card's UID is the same as the current

 doi:10.20944/preprints202507.1952.v1

session's. If so, the session is terminated. Cards with different UIDs are ignored while a session is active.

3.3. Secure Communication and Data Model

Communication between the PlugID devices and the central broker uses the MQTT protocol. The security of this communication, a critical point in any IoT deployment, is ensured by the implementation of **TLS (Transport Layer Security)**. On the server side, the mosquitto broker was configured to require TLS connections, using a set of digital certificates generated from a self-signed Certificate Authority (CA). This ensures that all data traffic between the devices and the server is encrypted, protecting against eavesdropping and man-in-the-middle attacks, in line with the best security practices recommended in the literature [18].

The data is formatted in JSON (JavaScript Object Notation), a lightweight and human-readable standard, ideal for interoperability. The payload structure varies slightly depending on the PlugID model but always contains detailed information about energy consumption. Table 3 presents examples of data payloads for the different models, demonstrating the richness and structure of the collected information.

Table 3. Data payloads for the different models.

Model	Example JSON Data Payload
PlugID-E	{ "Time":"2021-07-27T17:35:42", "ENERGY":{ "Total":0.008, "Power":12, "Voltage":128, "Current":0.168 } }
PlugID-E/AT	{ "Time":"2021-07-27T18:08:29", "RC522":{ "UID":"9996E8B8", "Type":"MIFARE 1KB" } } (in addition to energy data)
PlugID-ETH	{ "Time":"2021-07-27T17:35:42", "AM2301":{ "Temperature":29.2, "Humidity":48.5 }, "TempUnit":"C" } (in addition to energy data)
SM-3W Lite (AC)	{"variable":"PT", "value":79.33, "unit":"W"} {"variable":"IA", "value":6.92, "unit":"A"}

4. Case Study

To validate the feasibility and functionality of the PlugID platform, a deployment was carried out in a real-world test scenario. This scenario served as a proof of concept for the authenticated energy consumption paradigm.

4.1. Implementation of hardware, firmware, and software

The starting point for the development of an authenticated measurement model is a meter that has the ability to make the association between energy consumption and responsible for consumption. The unavailability of commercial meters - and even academic research - that contemplated an authenticated measurement model with data interoperability led to the development of our own meter, which we called PlugID.

PlugID was designed based on the following premises:

- Possibility of high granularity in the temporal aspect of energy consumption monitoring;
- Ease of connection to electrical outlets and circuits typical of homes and offices;
- Ability to identify the user responsible for energy consumption at each instant of time;
- Interoperability without relying on specific software applications to access consumer data.

The architectural overview of PlugID Platform can be seen in Figure 1. PlugID block diagram.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 July 2025 doi:10.20944/preprints202507.1952.v1

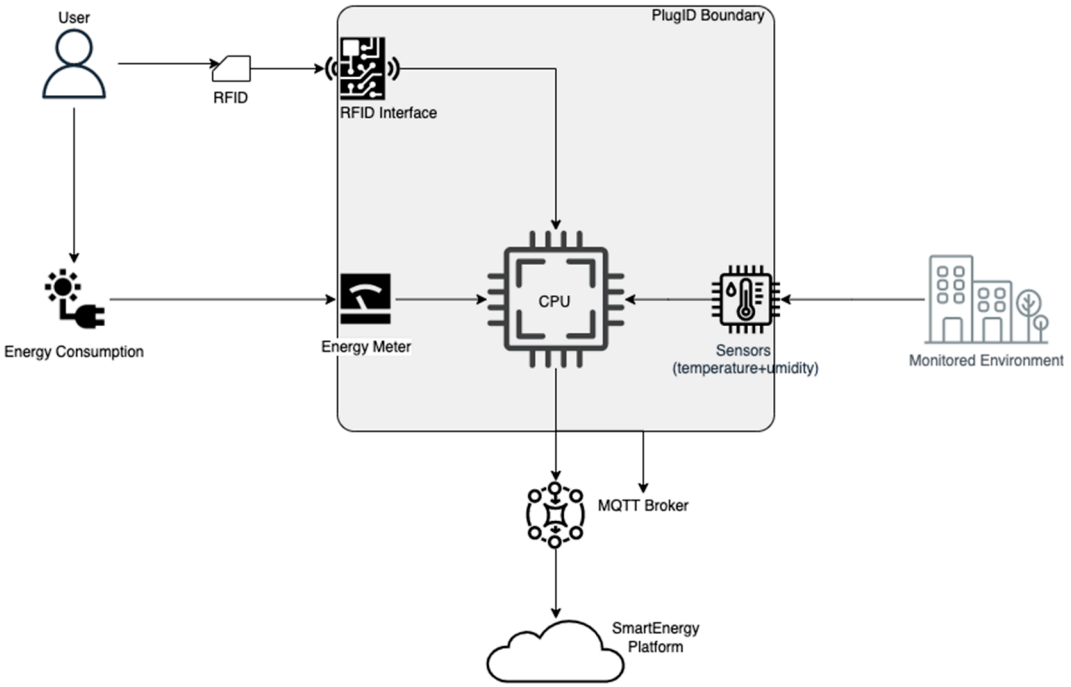
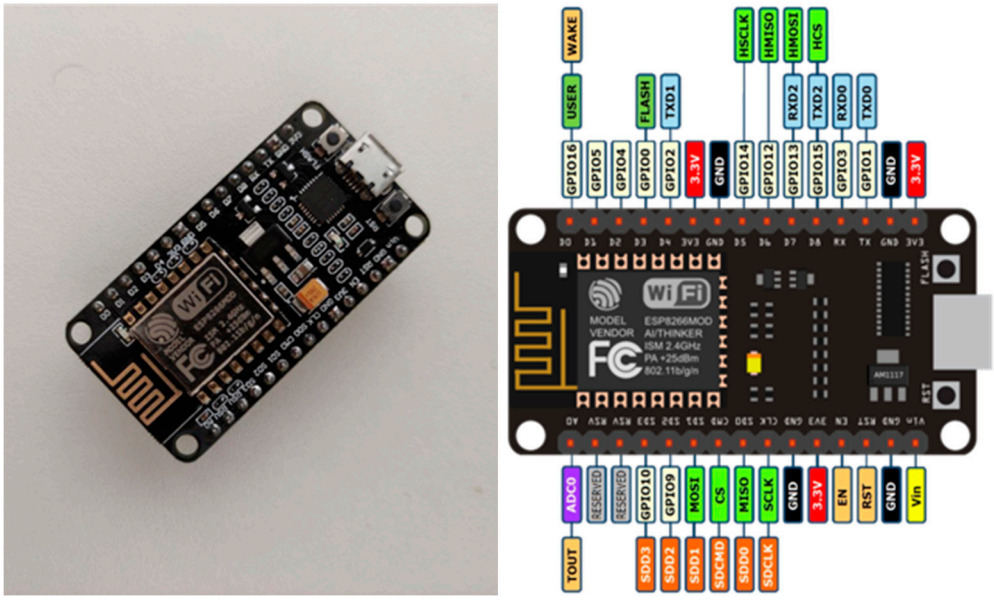


Figure 1. PlugID block diagram.

The starting point for the PlugID implementation was the selection of technologies for each of its modules/components.

Hardware / Central Processing Unit (CPU). Regarding the CPU, we opted for the ESP8266 microcontroller. It is a low-cost microcontrolled development environment with low power consumption characteristics. The ESP8266 is a microcontroller capable of Wi-Fi connection (as long as it has an antenna), not needing any external module to connect to Wireless networks. The chip is extremely cheap and is also available in module form (with integrated antenna) or as part of dev kits. The PlugID project uses the ESP8266 NodeMCU v2 - ESP12 board (Figure 2), which provides several interfaces and communication resources. The WiFi module ESP8266 NodeMCU is a development board that combines the ESP8266 chip, a usb-serial interface and a 3.3V voltage regulator. Programming can be done using LUA or the Arduino IDE, using communication via micro-usb cable. The NodeMCU has a built-in antenna and micro-usb connector for connection to the computer, in addition to 11 I/O pins and analog-to-digital converter, having remote firmware upgrade capabilities.



 doi:10.20944/preprints202507.1952.v1

Figure 2. ESP8266 NodeMCU (left) and connection diagram (right).

Measurement Module and Sensor. To measure energy consumption, the PZEM-004T Multifunction Electrical Monitoring Module (Figure 3) was chosen. The PZEM-004T has voltage, current and power measurement capacity, having been chosen for the possibility of indirect measurement, through a current terminal composed of a coil, which allows the measurement of electrical energy without the need for intervention in the electrical circuits under measurement.

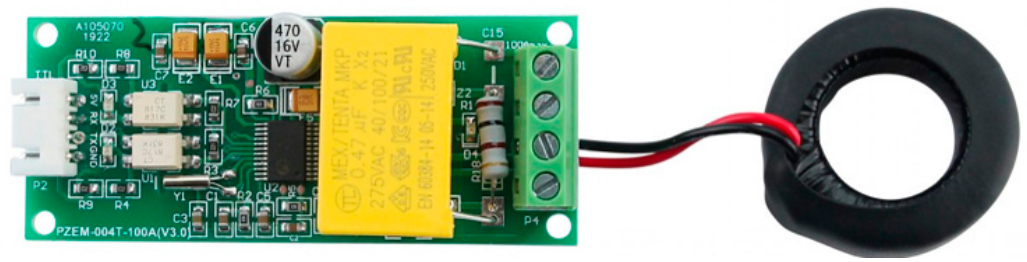


Figure 3. PZEM-004T Module already connected to the measuring coil.

User Authentication Module. User authentication in PlugID follows a token-based approach, through RFID (radio frequency identification) reading is the reference for user identification. The RFID reading is performed by the RFID Reader Module - RC522, developed by NXP (Figure 4).

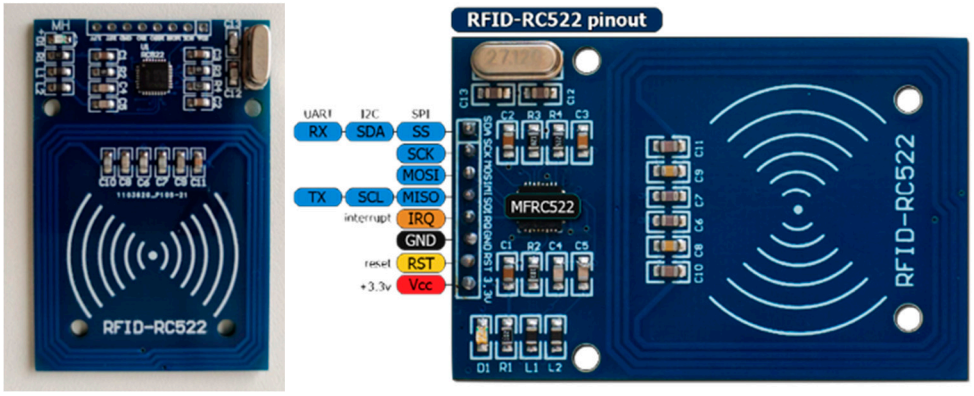
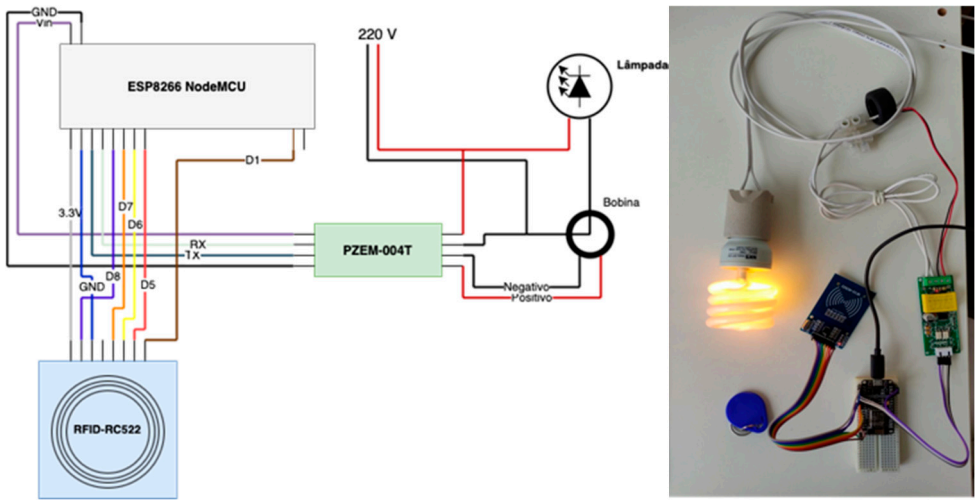


Figure 4. RFID - RC522 (left) and its connection diagram (right).

PlugID electrical diagram and first prototype. Figure 5 below shows the electrical diagram of PlugID and the first prototype used to demonstrate the operation of the project, while Figure 6 show PlugID in its operating box and already in operation.



 doi:10.20944/preprints202507.1952.v1

Figure 5. Electrical diagram of PlugID and first developed prototype.

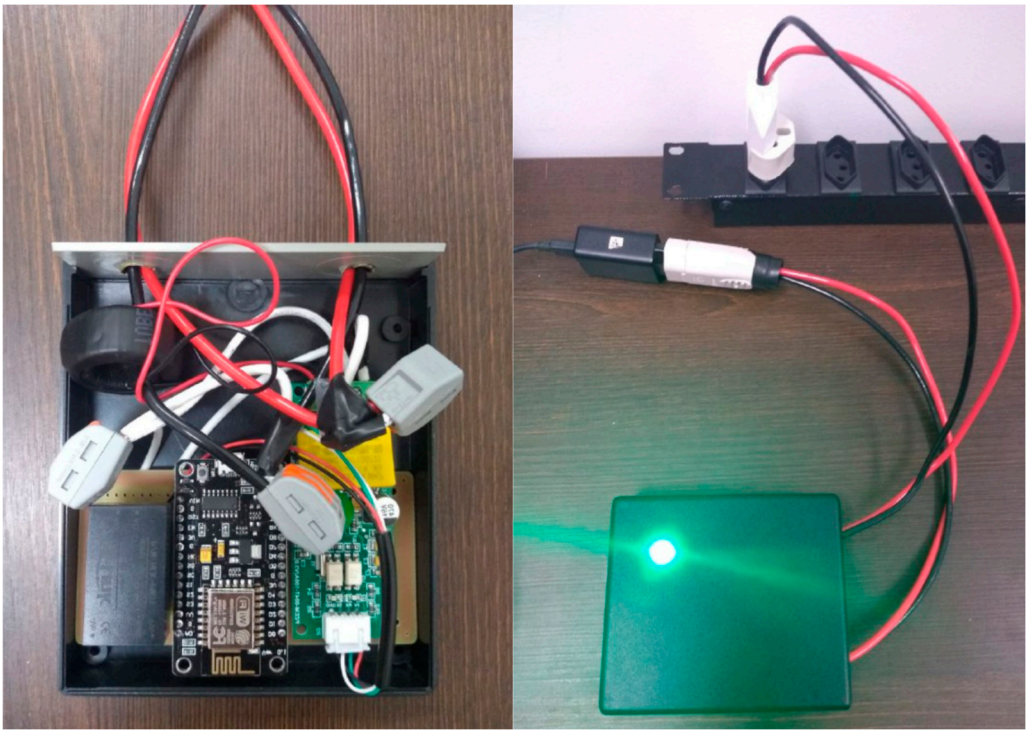


Figure 6. PlugID on its operating box.

Firmware. The firmware of the PlugID device is based on Tasmota (Figure 7), an open-source firmware for ESP8266-based devices, supporting MQTT and Over-the-Air (OTA) protocols.

Figure 7. TASMOTA electronic manual (readme).

Communications. To communicate the measured data, the MQTT protocol was used, which has become a standard for the communication of sensors, meters and Internet of Things devices. MQTT is a publisher-subscriber communication protocol that runs on top of TCP/IP. As in many publisher-subscriber protocols, the typical architecture (Figure 8) of an MQTT-based system demands the use of a *broker* that will be an intermediary between PlugID devices and other systems for collecting, centralizing, visualizing and analyzing the collected data.

 doi:10.20944/preprints202507.1952.v1

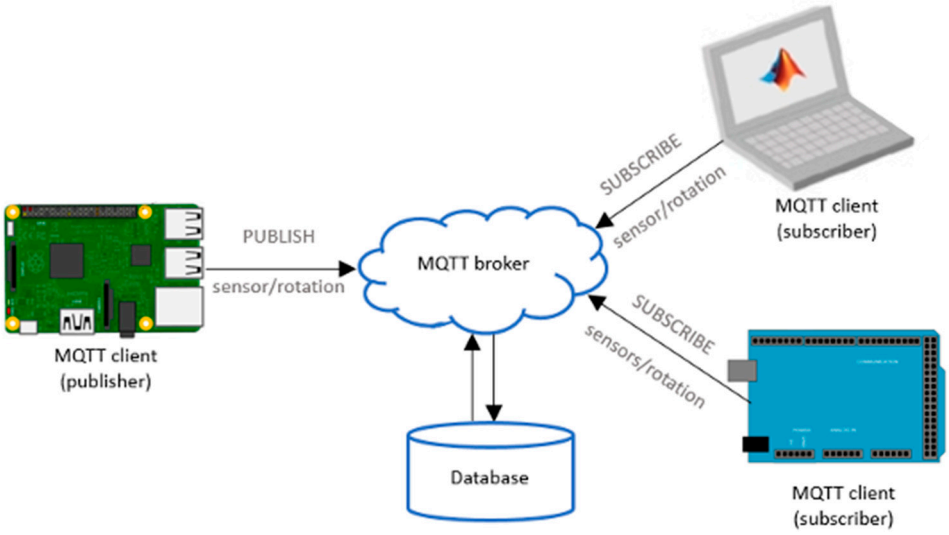


Figure 8. Basic model for data collection via MQTT broker.

MQTT Broker. After the proper configuration of the microcontrollers, it was possible to observe the energy consumption in the Tasmota console, along with information from the temperature and humidity sensor and the UID of an approximate card/token in the RFID reader, as can be seen in the following JSON:

```
{
"Time":"2021-07-27T17:35:42",
"ENERGY":{
"TotalStartTime":"2021-07-27T17:35:23",
"Total":0.008,
"Yesterday":0.000,
"Today":0.008,
"Frequency":60,
"Power":12,
"ApparentPower":22,
"ReactivePower":18,
"Factor":0.53,
"Voltage":128,
"Current":0.168
},
"AM2301":{
"Temperature":29.2,
"Humidity":48.5,
"DewPoint":17.2
},
"TempUnit":"C"
}
{
"Time":"2021-07-27T18:08:29",
"RC522":{
"UID":"9996E8B8",
"Data":"",
"Type":"MIFARE1KB"
}
}
```

In possession of these data, the MQTT (Message Queuing Telemetry Transport) protocol was used to send them to a server, which runs an MQTT broker called mosquitto. This application behaves as an agent for sent and received messages. MQTT works on a publisher/subscriber scheme, in which a publisher sends data to a typical in the MQTT broker, which is basically a channel. The subscriber then subscribes to the same typical and has access to this data. In the case of the project, the microcontrollers have the role of publishers, and on the server itself where the mosquitto service runs, the service also runs from a subscriber to collect all sent data, which arrives in the format of the JSONs shown above and then are saved in log files.

In the microcontrollers, TLS (Transport Layer Security) was configured, which is a protocol that encrypts all data emitted. In this way, MQTT on Tasmota has been configured with TLS support. There was extensive configuration also on the server side to run the mosquitto service with TLS, and several changes to the mosquitto configuration file were made.

 doi:10.20944/preprints202507.1952.v1

For the functioning of TLS in the mosquitto, a self-signed Certificate Authority was created, as well as its certificate and the certificate for the mosquitto. A CA can issue digital certificates, and each one contains an associated public key. In an asymmetric cryptography, it is possible to make use of the private and public keys to exchange a symmetric key, which will actually be used for data traffic. This process is performed automatically once the settings for TLS and certificates are properly defined.

4.2. Deployment Scenario

The chosen test environment was the office of Green Hat, a small company located in Rio de Janeiro. This environment represents an ideal use case: a shared workspace where the energy consumption of multiple users and equipment is traditionally aggregated.

A total of seven PlugID devices were deployed at strategic points in the office. The distribution of the different models was planned to cover various monitoring use cases:

- **PlugID-E/AT (with authentication):** Installed at shared workstations, where multiple employees could use the same computer at different times. RFID authentication was necessary to attribute consumption to the correct user.
- **PlugID-E (without authentication):** Used at fixed workstations, assigned to a single individual, where continuous authentication was considered unnecessary for the proof of concept.
- **PlugID-ETH (with environmental sensor):** Positioned in key locations to collect temperature and humidity data, allowing for the correlation between environmental conditions and energy consumption, especially of the air conditioning system.

In addition to the PlugID devices, the consumption of the air conditioning system, one of the largest energy consumers in the office, was monitored using a commercial **SM-3W Lite** meter. This meter was integrated into the same data collection platform via MQTT, although its communication was not encrypted with TLS, unlike the PlugID devices.

The demonstration scenario is shown in Figure 9.

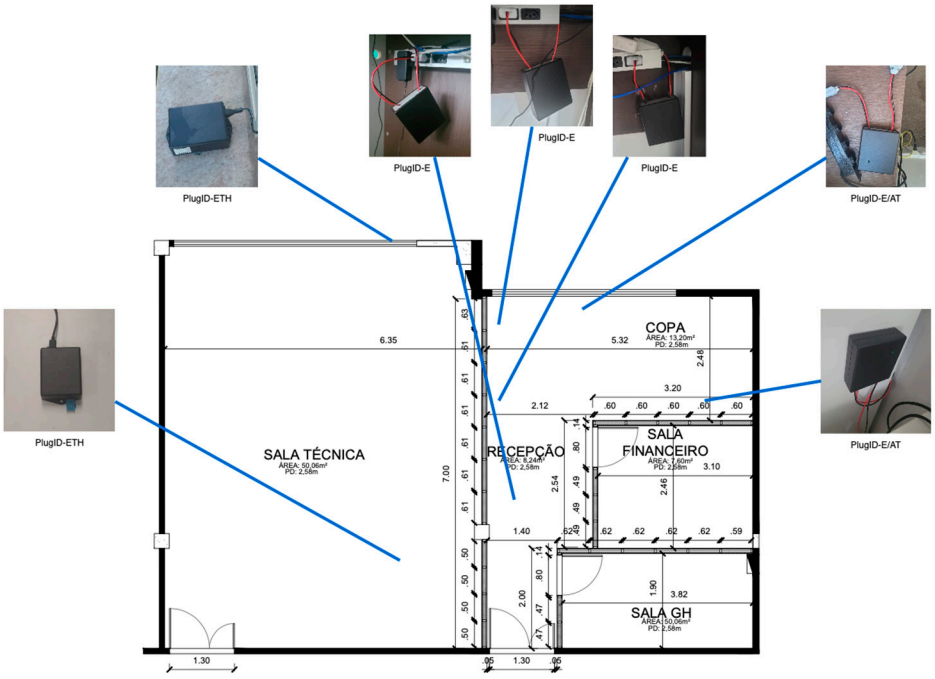


Figure 9. Small office where the devices were deployed.

 doi:10.20944/preprints202507.1952.v1

4.3. Data Collection and Visualization

Once deployed, the system began to continuously collect and transmit data to the SmartEnergy platform. The system's functionality could be observed through several interfaces:

- **Tasmota Web Console:** Each PlugID device offers a local web interface for real-time configuration and monitoring. Figure 7 shows an example of this interface, with instantaneous readings of power, voltage, current, and, in applicable models, temperature, humidity, and the UID of the last RFID session.
- **MQTT Broker:** On the server, raw data arrived as JSON messages, as per the examples in Table 3. This confirmed the correct data flow and proper formatting.
- **SmartEnergy Platform (Kibana):** The data ingested and stored in Elasticsearch was used to create interactive dashboards in Kibana. These dashboards, as exemplified in Figure 6, allowed for the visualization of energy consumption time series, the correlation of consumption peaks with authenticated user sessions, and the analysis of the impact of environmental factors on energy use.

The various PlugID devices installed in the test environment were interconnected through a computational platform called SmartEnergy with two general objectives:

- analyze energy consumption data;
- implement energy consumption policies.

The SmartEnergy is a cloud-based platform deployed over the Elastic Stack technology. Figures 10 and 11 show two views that are available for user of the SmartEnergy platform.

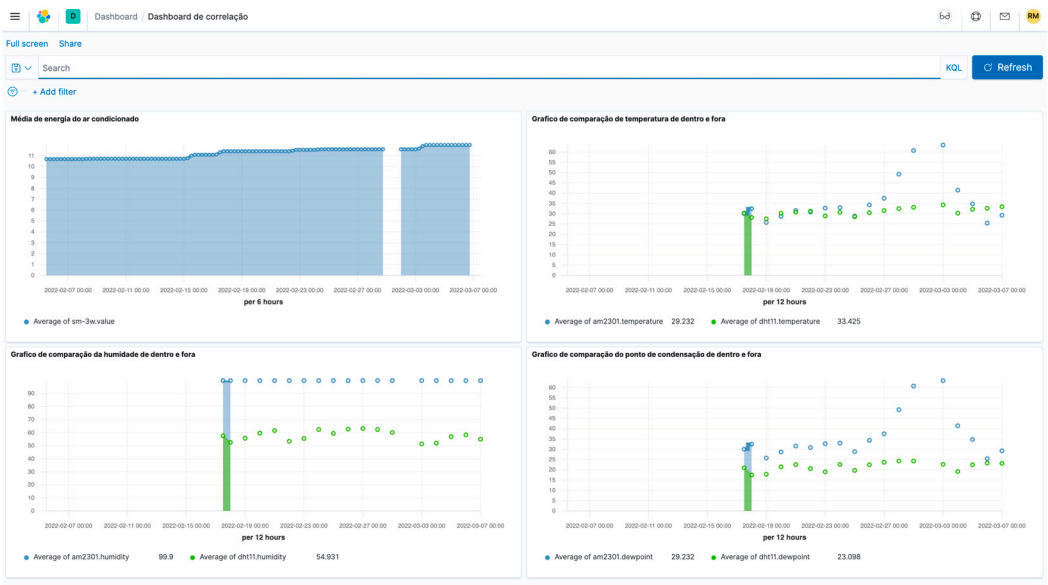


Figure 10. SmartEnergy dashboard.

 doi:10.20944/preprints202507.1952.v1

Figure 11. SmartEnergy "discovery" view.

4.4. Proof of Concept: Enabling Granular Energy Policies

The platform demonstrated its ability to go beyond simple monitoring by enabling the implementation of data-driven energy management policies. Two scenarios illustrate this potential:

1. **Accountability Scenario:** An office manager observes, through the SmartEnergy dashboard, a spike in energy consumption at a shared workstation over the weekend. Traditional aggregated consumption would only flag the event. With the PlugID platform, the manager can cross-reference the timestamp of the consumption peak with the RFID session logs. The system reveals that UID "9996E8B8" was logged in at that time, allowing the manager to identify the responsible user and initiate a targeted conversation about the policy for using equipment outside of working hours. This transforms an anonymous problem into a matter of personal responsibility.
2. **Active Access Control Scenario:** Based on the collected data, which shows a pattern of equipment being left on overnight, the company decides to implement a more active energy policy. Using the control capabilities of the PlugID (via its internal relay), a rule is configured on the SmartEnergy platform: all workstation outlets are automatically de-energized at 8:00 PM. Access after this time is only permitted if the user authenticates with an RFID token associated with a profile that has "after-hours access" privileges. This scenario demonstrates the transition from passive monitoring to active and dynamic access control, a key feature of advanced energy management systems.

5. Discussion

The implementation and demonstration of the PlugID platform provide a basis for discussing the broader implications of authenticated energy consumption. This section analyzes the potential impact on user behavior, critically evaluates the security and privacy of the solution, and outlines the study's limitations and directions for future work.

5.1. The Impact of Authentication on Energy-Related Behavior

The introduction of authentication into the energy consumption process represents a socio-technical intervention with the potential to fundamentally alter user behavior. The simple act of having to "swipe a badge" to turn on a computer or piece of equipment transforms energy use from a passive and invisible action into a conscious and deliberate act.

This mechanism can leverage well-established principles of behavioral science. First, the **Hawthorne effect**, which posits that individuals modify their behavior in response to the awareness

 doi:10.20944/preprints202507.1952.v1

of being observed. By knowing that their consumption is being measured and attributed, users are likely to become more conservative. Second, the power of **direct feedback**. The SmartEnergy platform can provide each user with a report of their personal consumption, making the impact of their actions tangible and measurable. This direct visibility is a much stronger motivator for change than generic appeals for conservation.

Although the project's scope did not include a formal behavioral study, a "perceptible change in the mindset of the functional staff regarding energy consumption" was observed at the Green Hat premises after the devices were deployed. While anecdotal, this observation serves as preliminary evidence that making energy consumption visible and attributable can, in fact, foster a culture of greater awareness and responsibility.

5.2. Security and Privacy Analysis of the PlugID Platform

A critical evaluation of the platform's security is essential. Table 4 presents a threat model, analyzing the platform's vulnerabilities in relation to threats identified in the literature and proposing mitigation strategies.

Table 4. Threats to PlugID respective mitigation strategies.

Threat Category	Specific Threat	Platform Vulnerability	Proposed Mitigation / Future Work
Communication Channel	Eavesdropping, Man-in-the-Middle	Interception of MQTT data in transit.	**Implemented:** Use of TLS to encrypt the MQTT channel, protecting data confidentiality and integrity.[18]
Device Authentication	Spoofing Attack	Cloning of RFID cards to gain unauthorized access.[14]	**Future Mitigation:** Implement Multi-Factor Authentication (MFA), such as RFID + PIN, or use more secure methods like smartphone-based authentication.
Physical Security	Node Tampering, Fake Node	An attacker with physical access can alter the PlugID's hardware/firmware or replace it with a malicious device.[11]	**Mitigation:** Implement cabinets with physical security seals. **Future Work:** Investigate the use of Physical Unclonable Functions (PUFs) for hardware attestation.
Availability	Denial of Service (DoS)	The centralized MQTT broker is a single point of failure and can be targeted by flooding attacks.[14]	**Future Mitigation:** Implement load balancing and traffic filtering mechanisms. Investigate decentralized or federated broker architectures.
Data Privacy	Activity Inference	Granular and authenticated consumption data can be used to monitor employee activities in detail.[16]	**Mitigation:** Implement strict data governance policies with access control to raw data. **Future Work:** Develop privacy-preserving aggregation and anonymization techniques for less granular analyses.

The analysis reveals a design with a solid security foundation, notably the use of TLS, which directly addresses the most common communication threats. However, like any real-world system, there are weaknesses. The reliance on RFID for authentication is a known vulnerability, and the physical security of the device is a prerequisite that is outside the scope of the electronic design. More importantly, the very nature of the platform—collecting granular and attributed data—creates an inherent privacy challenge. The solution to this is not only technological but also political, requiring

 doi:10.20944/preprints202507.1952.v1

transparent and ethical data governance to balance the need for accountability with the user's right to privacy.

5.3. Limitations and Future Directions

It is important to acknowledge the limitations of this work, which also point to promising avenues for future research. The main limitations are:

- **Scale**: The deployment was a small-scale proof of concept (seven devices in a single office). The scalability of the platform, both in terms of device management and data processing, was not tested in a large-scale deployment.
- **Duration**: The data collection period was relatively short, which prevents the extraction of statistically significant conclusions about long-term behavioral changes.
- **Focus**: The main objective of the project was the development and validation of the technological tool (the PlugID platform), rather than conducting a formal study of energy efficiency or behavior.

Based on these limitations, the following directions for future work are proposed:

- Longitudinal Behavioral Study: Conduct a large-scale, long-term deployment in different types of environments (e.g., offices, university labs, co-working spaces) to quantitatively measure the impact of authenticated consumption on energy savings and behavioral change.
- Enhanced Authentication: Integrate alternative and more secure authentication factors to overcome the limitations of RFID. This could include PINs entered on an attached keypad, biometric authentication, or, more pragmatically, authentication based on smartphone apps (via Bluetooth Low Energy or Wi-Fi).
- Advanced ABAC Policies: Develop and implement more complex, attribute-based energy access control policies on the SmartEnergy platform. For example, policies that grant different energy quotas to different user roles or that dynamically adjust access based on the time of day and the cost of grid energy.
- Integration with Building Management Systems (BMS): Explore the integration of the PlugID platform with existing commercial BMS. This would allow authenticated consumption data at the outlet level to be correlated with data from centralized systems (like HVAC and lighting), providing a truly holistic view of the building's energy use.

6. Conclusion

This work presented the conception, design, implementation, and demonstration of the PlugID platform, an end-to-end system that introduces and enables the paradigm of authenticated energy consumption. By developing a low-cost, open-protocol smart plug integrated with a secure analytics platform, we have demonstrated the feasibility of attributing energy consumption directly to individual users in shared environments.

The central contribution of this study is twofold. First, it proposes a conceptual shift in the approach to energy efficiency, moving the focus from purely technological solutions to a socio-technical model that incorporates user accountability as a primary driver for conservation. The fundamental argument is that by making energy consumption a visible, measurable, and attributable event, we can overcome the "tragedy of the commons" that prevails in shared energy environments.

Second, the work offers a detailed and validated technical design for a platform that implements this paradigm. The use of low-cost hardware, open-source firmware (Tasmota), and standard, secure communication protocols (MQTT over TLS) makes the PlugID solution replicable, auditable, and a viable alternative to the proprietary and closed systems that dominate the IoT market.

Although the study has limitations in terms of scale and duration, it establishes a solid foundation and opens promising avenues for future research, including large-scale behavioral studies and the development of more sophisticated energy access policies. Ultimately, the PlugID platform is not just a device, but a tool that enables new strategies for sustainable resource

 doi:10.20944/preprints202507.1952.v1

management, engaging the user not as a passive spectator, but as an active and responsible participant in the collective effort of energy conservation.

Author Contributions: The four authors contributed in all phases of the work, including conceptualization, methodology, software implementation validation, original draft preparation, review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Faperj - Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro, grant number E-26/010.000584/2017 SmartEnergy, and Finep - Financiadora de Estudos e Projetos, grant number 1488/22 PlatCiber. The APC was funded by Fundação Euclides da Cunha.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

ABAC	Attribute-Based Access Control
ACL	Access Control List
ADC	Analog-to-Digital Converter
BMS	Building Management System
CA	Certificate Authority
DAC	Discretionary Access Control
DoS	Denial of Service
ESP	Espressif Systems Platform
ETH	Environmental Temperature and Humidity (PlugID variant)
FDI	False Data Injection
GPIO	General-Purpose Input/Output
HVAC	Heating, Ventilation, and Air Conditioning
ILM	Intrusive Load Monitoring
IoT	Internet of Things
JSON	JavaScript Object Notation
MAC	Media Access Control (Address)
MFA	Multi-Factor Authentication
MQTT	Message Queuing Telemetry Transport
NILM	Non-Intrusive Load Monitoring
OTA	Over-The-Air (Firmware Update)
PUF	Physical Unclonable Function
RBAC	Role-Based Access Control
RFID	Radio-Frequency Identification
SPI	Serial Peripheral Interface
TLS	Transport Layer Security
UID	Unique Identifier

References

1. Poyyamozhi, M.; Murugesan, B.; Rajamanickam, N.; Shorfuzzaman, M.; Aboelmagd, Y. IoT—A Promising Solution to Energy Management in Smart Buildings: A Systematic Review, Applications, Barriers, and Future Scope. *Buildings* **2024**, *14*, 3446. https://doi.org/10.3390/buildings14113446
2. Pu, Z., Huang, Y., Weng, M., Meng, Y., Zhao, Y., & He, G. (2024). Enhancing non-intrusive load monitoring with weather and calendar feature integration in DAE. *Frontiers in Energy Research*, *12*, 1361916. https://doi.org/10.3389/fenrg.2024.1361916
3. Zhao Q, Liu W, Li K, Wei Y, Han Y. Unknown appliances detection for non-intrusive load monitoring based on vision transformer with an additional detection head. Heliyon. 2024 May 7;10(9):e30666. doi: 10.1016/j.heliyon.2024.e30666. PMID: 38765156; PMCID: PMC11101768.

 doi:10.20944/preprints202507.1952.v1

4. Mensah, Nobert & Abdel-Fatao, Hamidu & Yao, Yevenyo & Yevenyo Ziggah, Yao & Nunoo, Solo. (2024). An Effective Non-Intrusive Load Monitoring (NILM) for Residential Appliances using Wavelet Transform and Clustering. International Journal of Computer Applications. 186. 975-8887. 10.5120/ijca2024923901.
5. Shabbir, N.; Vassiljeva, K.; Nourollahi Hokmabad, H.; Husev, O.; Petlenkov, E.; Belikov, J. Comparative Analysis of Machine Learning Techniques for Non-Intrusive Load Monitoring. *Electronics* **2024**, *13*, 1420. https://doi.org/10.3390/electronics13081420
6. Condon F, Martínez JM, Eltamaly AM, Kim YC, Ahmed MA. Design and Implementation of a Cloud-IoT-Based Home Energy Management System. Sensors (Basel). 2022 Dec 24;23(1):176. doi: https://doi.org/10.3390/s23010176. PMID: 36616774; PMCID: PMC9824460
7. Ahsan, M.S.; Pathan, A.-S.K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art. *IoT* **2025**, *6*, 9. https://doi.org/10.3390/iot6010009
8. Almarri, Seetah & Frikha, Mounir. (2024). Authentication and Access Control Mechanisms to Secure IoT Environments: A comprehensive SLR. 10.20944/preprints202405.0948.v1.
9. Ali, Inayat & Sabir, Sonia & Ullah, Zahid. (2024). Internet of Things Security, Device Authentication and Access Control: A Review.
10. Ragothaman K, Wang Y, Rimal B, Lawrence M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. Sensors (Basel). 2023 Feb 6;23(4):1805. doi: https://doi.org/10.3390/s23041805. PMID: 36850403; PMCID: PMC9963042.
11. Nambundo, J.M.; de Souza Martins Gomes, O.; de Souza, A.D.; Machado, R.C.S. Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review. *Energies* **2025**, *18*, 1445. https://doi.org/10.3390/en18061445
12. Abdalzaher, M.S.; Fouda, M.M.; Emran, A.; Fadlullah, Z.M.; Ibrahem, M.I. A Survey on Key Management and Authentication Approaches in Smart Metering Systems. *Energies* **2023**, *16*, 2355. https://doi.org/10.3390/en16052355
13. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*, 5894. https://doi.org/10.3390/en14185894
14. Kua, J.; Hossain, M.B.; Natgunanathan, I.; Xiang, Y. Privacy Preservation in Smart Meters: Current Status, Challenges and Future Directions. *Sensors* **2023**, *23*, 3697. https://doi.org/10.3390a
15. Zhang, X.-Y.; Kuenzel, S.; Córdoba-Pachón, J.-R.; Watkins, C. Privacy-Functionality Trade-Off: A Privacy-Preserving Multi-Channel Smart Metering System. *Energies* **2020**, *13*, 3221. https://doi.org/10.3390/en13123221
16. Díaz Redondo, R.P.; Fernández-Vilas, A.; Fernández dos Reis, G. Security Aspects in Smart Meters: Analysis and Prevention. *Sensors* **2020**, *20*, 3977. https://doi.org/10.3390/s20143977.