

Smart home system with real-time hybrid notification framework

Ryan Fikri¹, Agariadne Dwinggo Samala², Gustia Fernando², Soha Rawas³

¹Department of Electronic Systems Engineering Technology, Faculty of Engineering, Universitas Negeri Padang, Padang, Indonesia

²Department of Informatics Engineering Education, Faculty of Engineering, Universitas Negeri Padang, Padang, Indonesia

³Department of Mathematics and Computer Science, Faculty of Science, Beirut Arab University, Beirut, Lebanon

Article Info

Article history:

Received Nov 25, 2025

Revised Aug 24, 2026

Accepted Sep 4, 2026

Keywords:

Automation system

Blynk platform

Energy monitoring

ESP32

Radio frequency identification access

Smart home internet of things

WhatsApp alert

ABSTRACT

Smart home systems are increasingly adopted for residential energy monitoring, automation, and access security; however, many implementations treat these functions separately, limiting operational coordination and timely user response. This study developed an ESP32-based prototype integrating environmental and electrical sensing, relay-based load control, radio frequency identification (RFID) technology authentication, token management, and two user communication channels. Blynk was configured for continuous monitoring and remote control, whereas WhatsApp conveyed event-specific security, overload, and token messages. The distinguishing contribution was not the use of either service alone, but their coordination with sensing, authentication, protection, and control within one operational workflow. Functional laboratory evaluation covered network initialization, sensor response, six load scenarios, RFID authorization states, token logic, and message delivery. Wi-Fi initialized within 2–5 s, WhatsApp messages were observed within 1–2 s, recorded line voltage ranged from 216 to 221 V, and the expected response occurred in all six scenarios, including protective disconnection above 3.5 A. The results establish the laboratory-scale feasibility of coordinated household monitoring, control, authentication, and event escalation, while field reliability, measurement accuracy, security, and interoperability require further validation.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ryan Fikri

Department of Electronic Systems Engineering Technology, Faculty of Engineering

Universitas Negeri Padang

St. Prof. Dr. Hamka, Kampus Air Tawar, Padang, Sumatera Barat, 25131, Indonesia

Email: ryanfikri@ft.unp.ac.id

1. INTRODUCTION

As households become more dependent on electronic appliances for comfort, security, and daily activities, residential electricity consumption continues to increase. Effective energy monitoring and management are therefore essential to reduce waste, improve reliability, and support sustainable living. Recent advances in internet of things (IoT) technology have enabled smart home systems to collect real-time data, monitor environmental conditions, and control connected devices more efficiently [1]–[6]. These developments highlight the need for smart home solutions that are reliable, responsive, and accessible to household users.

Despite this progress, many existing smart home systems remain functionally fragmented. Energy-monitoring prototypes commonly report electrical variables but do not coordinate monitoring with automated protection, event escalation, and household access control. Other systems rely on a single dashboard that requires active user attention, while security-focused architectures may add computational or deployment

complexity. Transmission delay and secure authentication are therefore not independent concerns: a delayed or unnoticed overload or access event reduces the operational value of otherwise accurate monitoring [7]–[11].

Recent studies have advanced ESP32-based monitoring, microcontroller automation, connected sensing, fog-based energy management, and secure smart-home architectures [12]–[18]. For example, El-Khozondar *et al.* [9] combined ESP32 energy monitoring with Blynk and WhatsApp, but centered the workflow on energy reporting. Other studies emphasize cloud scalability [10] or security mechanisms [11]. A remaining practical gap is the coordination of electrical and environmental sensing, relay-based protection, radio frequency identification (RFID) technology access state, token logic, and event-specific user communication within one low-cost household control loop.

Accordingly, the contribution of this study is architectural and operational, not the invention of an individual sensor or communication service. Blynk is assigned to continuous state visibility and remote control, whereas WhatsApp is assigned to event escalation for unauthorized RFID use, overcurrent, token thresholds, and token transactions. The distinguishing element is the explicit mapping from one detected event to its local control action, dashboard state, and message pathway. This system-level coordination differentiates the prototype from energy-reporting implementations that use similar communication tools [9].

This study makes three contributions. First, it specifies and implements a low-cost control loop that connects environmental and electrical sensing, two relay-controlled loads, RFID authentication, token state, and protective actuation. Second, it defines complementary notification roles for continuous dashboard supervision and event-specific messaging. Third, it evaluates operational feasibility through predefined functional checks covering connectivity, sensing response, six load scenarios, RFID states, token logic, and message delivery. The evaluation supports prototype feasibility under the reported laboratory conditions; it is not presented as a long-term reliability or metrological-accuracy study.

2. METHOD

This study adopted an experimental prototyping approach combining hardware-software co-design, staged module verification, system integration, and performance validation. The process began with functional requirement definition and architecture design, followed by electronic assembly and ESP32 firmware implementation. Each subsystem was checked independently before full integration. The complete prototype was then evaluated for power-supply stability, sensor response, load-control behavior, authentication operation, Wi-Fi initialization, and notification delay. This approach is consistent with experimental development practices used in IoT and embedded-system prototypes [11], [19]–[22].

2.1. Needs analysis

The system was designed to address the need for integrated residential monitoring, automated control, and secure user interaction. In practical operation, a smart home platform should monitor electrical and environmental conditions, provide timely feedback, control devices, and restrict unauthorized access [1]–[11]. The analysis therefore defined six requirements: environmental and electrical sensing, device control, secure authentication, event notification, remote monitoring, and reliable communication. Table 1 states the operational purpose of each requirement and Figure 1 shows how the corresponding modules exchange data and commands.

2.2. Hardware design

The hardware architecture is centered on the ESP32 microcontroller, selected for its integrated Wi-Fi capability and suitability for real-time IoT applications [12]–[18]. The sensing subsystem uses a DHT11 sensor for temperature and humidity, a ZMPT101B module for AC voltage, and an ACS712 sensor for load current. An RC522 module supports RFID authentication, while relay modules switch the lighting and air-conditioning loads according to the control logic. Regulated 3.3 V and 5 V supply lines were used for stable sensing and switching. Table 2 lists the components, and Figure 2 shows the physical interconnection that allows the ESP32 to coordinate sensing, access verification, and actuation.

Table 1. System requirements and the operational functions used to evaluate the integrated framework

Requirement type	Description
Environmental sensing	Measure temperature, humidity, AC voltage, and load current.
Device control	Provide automated and manual control of lighting and air-conditioning loads.
Secure authentication	Verify user identity through RFID before normal operation.
Real-time notification	Issue immediate alerts for threshold, overload, access, or transaction events.
Remote monitoring	Display current system parameters and load status on a mobile dashboard.
Communication reliability	Maintain Wi-Fi/cloud synchronization and consistent data exchange.

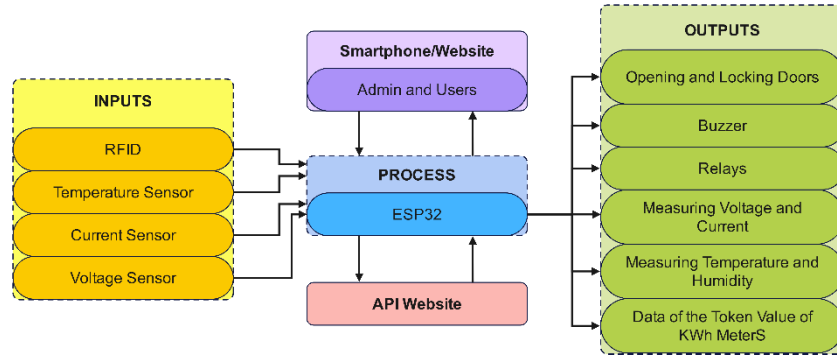


Figure 1. Functional architecture of the proposed system; readers should follow the sensor data toward the ESP32 and the resulting control, authentication, dashboard, and alert outputs

Table 2. Hardware modules and the specifications governing sensing, authentication, and load switching

Component	Function	Key specifications
ESP32	Main controller	Wi-Fi integrated, dual-core MCU
DHT11	Temp-humidity measurement	Range: 0-50 °C, 20-90 percent RH
ZMPT101B	AC voltage sensing	Range: up to 250 V AC
ACS712	Current sensing	Sensitivity: 185 mV/A (5 A version)
RC522 RFID	Authentication	13.56 MHz reader
Relay module	Device switching	5 V input, 10 A load capacity

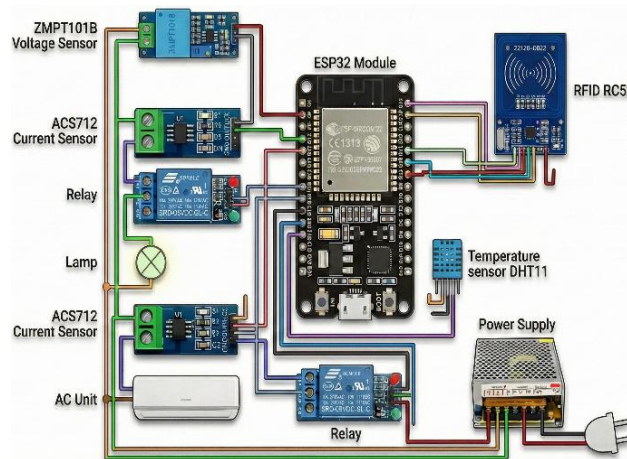


Figure 2. Hardware interconnection used in the prototype; the diagram identifies the ESP32 pins linking the sensing, RFID, and relay subsystems

2.3. Software design

The software architecture is organized into three interacting layers. Embedded firmware developed in Arduino IDE acquires sensor values, checks RFID and token states, evaluates thresholds, and controls the relays and buzzer. A communication layer exchanges dashboard data and routes event messages, following established IoT connectivity, middleware, server-platform, and cloud-security principles [23]–[28]. At the interface layer, Blynk supports continuous monitoring and remote control, whereas WhatsApp carries event-specific alerts and token-transaction feedback. These services are treated as complementary implementation channels rather than as newly introduced technologies.

The main operating logic is summarized in Algorithm 1 and Figure 3. Both representations apply the configured 3.5 A overcurrent threshold and distinguish the monitoring, authentication, protection, token, and top-up branches. This alignment makes the relationship between the implemented checks and their corresponding control and notification actions explicit.

Algorithm 1 formalizes the workflow in Figure 3. Its declared inputs, outputs, thresholds, and branch actions provide a reproducible description of the implemented control logic without implying unreported source-code or timing measurements.

Algorithm 1. Main control and notification workflow

Input: DHT11, ZMPT101B, and ACS712 readings; RFID UID; token state T; $I_{\max}=3.5$ A; configured T_{low} ; top-up code; Wi-Fi/Blynk state

Output: dashboard values; relay and buzzer states; WhatsApp messages; updated token state T

```

1 Initialize the ESP32, sensors, RFID reader, relays, buzzer, Wi-Fi, Blynk, and WhatsApp
  services.
2 WHILE the prototype is powered DO
3   IF Wi-Fi or Blynk is disconnected THEN
4     Reconnect and retry.
5   END IF
6   Acquire temperature, humidity, voltage V, current I, RFID state, and token state T.
7   Compute  $P = V \times I$ , update T using (1), and publish values and load states to Blynk.
8   IF an RFID card is detected THEN
9     IF the UID is authorized THEN retain the current operating state.
10    ELSE disable the designated loads and send a security alert.
11  END IF
12 END IF
13 IF  $I > I_{\max}$  THEN
14   Activate the buzzer, disable the affected load, and send an overcurrent alert.
15 END IF
16 IF  $T \leq 0$  THEN
17   Disable the designated high-power load and send a token-depletion alert.
18 ELSE IF  $T \leq T_{\text{low}}$  THEN send a low-token warning.
19 END IF
20 IF a top-up request is received THEN
21   IF the code is valid and unused THEN add credit, mark it used, and confirm.
22   ELSE reject the code and report its status.
23 END IF
24 END IF
25 Wait until the next 5 s monitoring cycle.
26 END WHILE

```

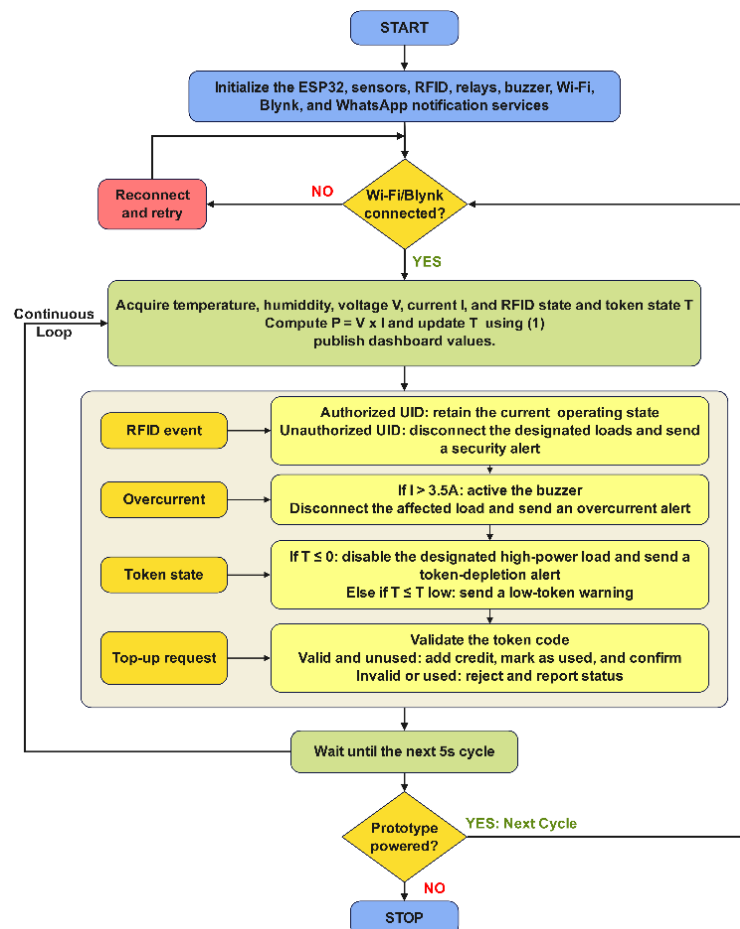


Figure 3. Control and notification workflow of the proposed prototype

2.4. Prototype development and integration

Prototype development proceeded in stages. Each module was first tested independently before the sensing, control, authentication, and communication components were integrated into one platform [10], [12]–[18]. The ESP32 firmware then executed control and notification routines in response to measured values, threshold conditions, and RFID outcomes. The assembled prototype was evaluated through connectivity, sensing, load-response, authentication, and token-notification tests. Figure 4 identifies the physical modules used in this controlled laboratory-scale implementation; the label “PLN electricity” denotes the Indonesian public-utility mains supply.

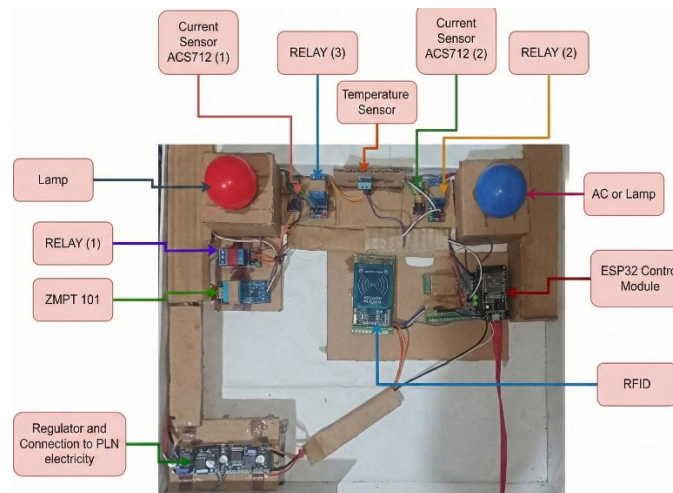


Figure 4. Laboratory-scale prototype used for functional validation

2.5. Experimental protocol and validation strategy

Validation was conducted as a functional bench assessment under controlled laboratory conditions. The testbed comprised a lamp and an air conditioner as controlled loads, DHT11, ZMPT101B, and ACS712 sensors, an RFID reader, relays, a buzzer, the Blynk dashboard, and event-triggered WhatsApp notifications. The assessment covered sensing, connectivity, authentication, load control, token management, and notification functions. Its purpose was to verify the integration and expected operation of the prototype under predefined conditions rather than to estimate statistical reliability.

The sensor outputs were used as control inputs and interpreted as functional prototype readings. The available experimental record does not include paired measurements obtained using traceably calibrated reference instruments or a formal repeated-sample design. Therefore, this study does not claim metrological accuracy, measurement uncertainty, precision, or repeatability for the DHT11, ZMPT101B, and ACS712 measurements.

Wi-Fi initialization time was operationally defined as the interval between system power-up and confirmation of network connectivity. Notification delay was defined as the interval between an event trigger and receipt of the corresponding WhatsApp message. The Blynk monitoring and token-processing loop used a 5 s update interval. Authentication was evaluated using authorized and unauthorized RFID states. Load-control validation covered six predefined scenarios: lamp-only operation, air-conditioner-only operation, rapid switching, simultaneous operation of both loads, zero-load operation, and an overcurrent condition above 3.5 A. Each electrical-scenario outcome was compared with its corresponding expected functional response. Because the available record does not provide a formal repeated-trial denominator, the results are reported as observed ranges and functional outcomes rather than statistical success rates.

Accordingly, the findings support the technical feasibility and internal operation of the integrated prototype under the reported laboratory conditions. They should not be interpreted as evidence of sensor accuracy, long-term reliability, or performance under population-scale or real-world residential deployment.

3. RESULTS AND DISCUSSION

This section evaluates connectivity, sensor and electrical response, six load scenarios, token-based control, and hybrid notification behavior. The findings are interpreted as functional evidence from the reported laboratory setup and are compared with the design emphasis of related smart-home research.

3.1. Connectivity and system initialization performance

Across the recorded connectivity checks, the ESP32 established Wi-Fi connectivity within 2–5 s and maintained communication with the cloud service and Blynk under normal network conditions. Temporary signal fluctuations did not interrupt the observed dashboard updates or WhatsApp delivery. This behavior is consistent with connected microcontroller applications [12]–[18] and supports prototype-scale monitoring [19]–[22]. Persistent loss, congested networks, and long-duration availability were not evaluated.

3.2. Sensor measurement and electrical parameter evaluation

The DHT11 produced temperature and humidity readings used as functional environmental inputs. In the electrical scenarios, the ZMPT101B output corresponded to line-voltage values of 216–221 V and the ACS712 output changed with load switching. Table 3 documents the configured supply rails and ESP32 pin allocation; it is not a calibration table. Together, these observations show that the controller distinguished the intended prototype states.

The available dataset supports comparison among operating states but does not support an accuracy percentage, uncertainty estimate, or long-term drift claim. Current and voltage values are therefore used only to describe the six functional scenarios in Table 4. A separate calibration study with a traceable reference instrument and repeated paired observations would be required before reporting measurement accuracy.

Table 3. Module supply requirements and ESP32 pin allocation used in the prototype

Sensor	Pin connections (ESP32)	Nominal supply (V)	Information
RFID	D21 (SDA)	3.3	Serial data (SDA) for communication with RFID operates at a voltage of 3.3 V
	D18 (SCK)	3.3	Serial clock (SCK) is used to synchronize communication with RFID
	D23 (MOSI)	3.3	Master out slave in (MOSI) for sending data to RFID
	D19 (MISO)	3.3	Master in slave out (MISO) is used to receive data from RFID
	D22 (RST)	3.3	Reset pin for RFID
DHT11	D12 (I/O)	3.3	The I/O pin on the DHT11 is used for measuring temperature and humidity
ZMPT101B	D36 (VP)	5	The ZMPT101B AC voltage sensor is connected to the analog pin to read the voltage signal.
ACS712	D34 (I/O)	5	ACS712 to measure electric current, with an analog output on D34
	D35 (I/O)	5	Analog pin addition to read the signal from ACS712
Relay	D14 (I/O)	5	Input/output pin for controlling a relay
	D25 (I/O)	5	Additional pin control for the relay
	D26 (I/O)	5	Additional control pin for relay

Table 4. Scenario-based validation linking each electrical condition to the expected and observed sensing, control, and protection response

Scenario	Expected behavior	Observed response	Result
Lamp ON	Detect low load (0.2–0.4 A); stable voltage	0.32 A; 219–221 V	PASS
AC ON	Detect high load (2.0–3.0 A); possible small voltage drop	2.47 A; 216–218 V	PASS
Rapid lamp/AC switching	Update within one 5 s cycle	0.30–2.51 A; status updated	PASS
Dual load ON	Sum current and recalculate power	2.79 A at 217 V; power recalculated	PASS
All loads OFF	Return current to baseline	0.00–0.03 A at 220 V	PASS
Overcurrent >3.5 A	Buzzer, alert, and load disconnection	All three actions executed	PASS

Overall, the sensing subsystem was adequate for distinguishing the operating states required by the prototype. This functional result does not establish measurement accuracy, uncertainty, or long-term stability.

3.3. Energy monitoring, load detection, and automation behavior

Table 4 summarizes the six load scenarios used to evaluate current detection, load-state identification, and automated controller responses. Lamp-only operation produced a current of 0.32 A at 219–221 V, whereas the air-conditioner load produced 2.47 A at 216–218 V. During rapid switching, the measured current changed from 0.30 A to 2.51 A within one 5 s monitoring cycle. Simultaneous operation of both loads produced 2.79 A at 217 V, while the zero-load condition produced readings within a 0.00–0.03 A noise range at 220 V. These observations indicate that the controller distinguished the predefined operating states and updated the calculated power value within the configured monitoring interval.

The overcurrent scenario demonstrated the operation of the integrated protection logic. When the measured current exceeded the configured threshold of 3.5 A, the controller activated the buzzer, sent a WhatsApp warning, and disconnected the load. The important functional outcome was the coordination of

three responses to the same detected event: local warning, remote notification, and protective load disconnection. Compared with conventional IoT arrangements that primarily emphasize monitoring, this coordinated response extends the prototype toward event-driven and safety-oriented automation [19], [21], [22], [26], [27].

The controller produced the expected functional response in each of the six recorded scenarios presented in Table 4. However, the available experimental record does not specify the number of repeated trials conducted for each scenario. The findings are therefore reported as functional outcomes and should not be interpreted as statistical success rates or evidence of long-term operational reliability.

3.4. Token-based control and notification response

Token control was evaluated through depletion, warning, replenishment, and event-notification scenarios. The remaining credit decreased with the computed power value and was synchronized with the 5 s monitoring loop. A low-token state generated a warning, whereas depletion disabled designated loads. The bounded prototype update rule is given in (1):

$$T_t = \max(0, T_{t-1} - kP_t) \quad (1)$$

where T_t is the remaining token state after monitoring cycle t , T_{t-1} is the preceding token state, P_t is the instantaneous power, and k is the conversion factor applied during one 5 s interval. The max operator prevents a negative state. Because k is a prototype parameter and was not derived from a utility tariff, the equation represents internal token logic rather than billing or revenue-grade energy metering.

Figure 5 illustrates the complementary roles of the hybrid interface. Figure 5(a) shows the Blynk dashboard used for continuous monitoring and remote load control, whereas Figure 5(b) shows the WhatsApp security notification issued after an unauthorized-access event and the resulting protective shutdown. The communication functions associated with these panels are summarized in Table 5.

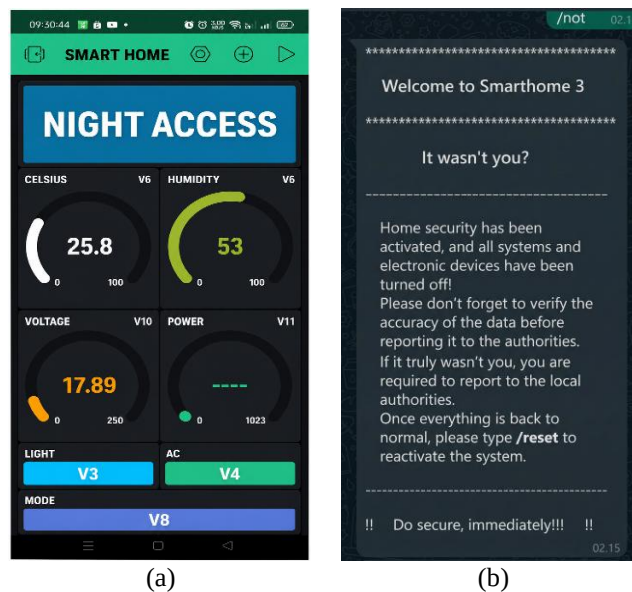


Figure 5. Hybrid interface roles; (a) Blynk for monitoring and control and (b) WhatsApp for security alerts

Table 5. Configured communication roles and observed response timing for the WhatsApp-only, Blynk-only, and hybrid pathways in the prototype

Configuration	Initialization	Feedback time	Dashboard	Remote control	Push alert	Security report	Token feedback	Coverage
WhatsApp only	2-5 s	1-2 s	No	No	Yes	Yes	Yes	3/5
Blynk only	2-5 s	<=5 s refresh	Yes	Yes	Not enabled	Not enabled	Dashboard only	2/5
Hybrid (proposed)	2-5 s	1-2 s alert; <=5 s dashboard	Yes	Yes	Yes	Yes	Yes	5/5

Figure 6 presents the token transaction feedback path. Figure 6(a) shows the purchase form used to initiate the top-up request, whereas Figure 6(b) shows the WhatsApp confirmation containing the invoice, transaction status, timestamp, and generated token code. This implementation follows broader IoT requirements for connectivity, middleware, service integration, and secure communication [24]–[31]. The observed result shows functional feasibility under normal network conditions; diverse appliances, intermittent networks, and production payment security were outside the test scope.

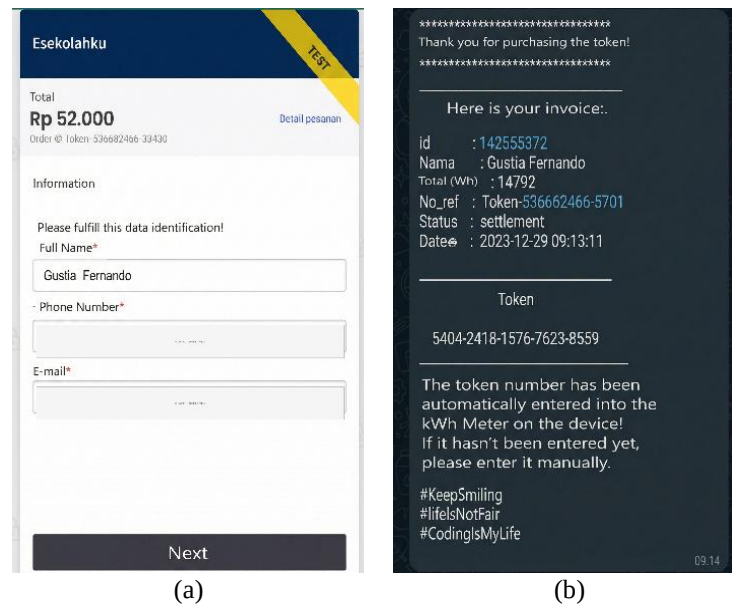


Figure 6. Token transaction feedback path; (a) the purchase form captures the top-up request, and (b) WhatsApp returns the invoice, status, timestamp, and token information

3.5. Comparative feature analysis of notification and control platforms

To examine the contribution of hybrid communication, the implemented WhatsApp and Blynk pathways were considered separately and together. Table 5 reports functions enabled in this prototype and must not be read as a comparison of the maximum capabilities of either platform. The functional coverage count includes continuous dashboard monitoring, remote device control, immediate event notification, security-event reporting, and token-transaction feedback.

In the tested configuration, WhatsApp carried event and transaction messages but did not provide persistent monitoring or direct device control. Blynk supplied dashboard monitoring and control with a refresh interval of up to 5 s; push escalation was not enabled on that pathway. Combining the configured channels therefore covered all five implemented functions: urgent events were observed within 1–2 s, while routine state information and control remained available through the dashboard. This is an implementation-specific result, not a universal ranking of the two services.

3.6. Discussion and implications

Table 6 positions the framework relative to recent smart-home studies. Esposito *et al.* [10] emphasize cellular IoT and serverless scalability. El-Khozondar *et al.* [9] are the closest communication comparison because their ESP32-based energy monitor also uses Blynk and WhatsApp. The difference claimed here is narrower: the present control loop additionally couples RFID state, token state, a 3.5 A protection rule, relay actuation, and event-specific routing. Ramachandra and Natarajan [32] address multi-dwelling energy management, whereas Umer *et al.* [33] emphasize blockchain and learning-based security. Thus, the study contributes coordinated household operation rather than a new messaging channel or a superior sensing method.

The observed behavior supports this limited integration claim. A 2–5 s initialization interval established the connected state; the 5 s loop updated routine monitoring; WhatsApp messages were observed within 1–2 s; and the overcurrent scenario linked a value above 3.5 A to buzzer activation, a user warning, and load disconnection. These functions cover consecutive stages of one event chain—detection, decision,

actuation, and communication—without implying superior sensor accuracy or network performance beyond the test conditions.

Table 6. Evidence-based positioning of the proposed framework relative to recent monitoring, communication, scalability, and security approaches

Ref.	Approach	Communication/monitoring	Security/control emphasis	Primary contribution
[9]	ESP32 energy monitoring	Blynk and WhatsApp	No integrated RFID authentication	Low-cost residential energy monitoring
[10]	Cellular IoT, MQTT, and serverless cloud	NB-IoT and MQTT	No household RFID control	Scalable cloud-connected architecture
[32]	Home energy management	Multi-dwelling real-time monitoring	Not centered on user authentication	Scalability across dwellings
[33]	Blockchain and deep learning	Intelligent automation	Blockchain device authentication	Security and AI-assisted automation
Proposed	Integrated ESP32 framework	Blynk dashboard plus WhatsApp alerts	RFID, token control, and overload disconnection	Coordinated household monitoring, control, access, and escalation

In practical terms, the coordinated event chain links an abnormal condition to local action and user awareness while preserving dashboard supervision. RFID adds an authorization state, and token feedback links the computed load state to a user-facing credit mechanism. The low-cost components and familiar interfaces are relevant to household prototyping. Regional monitoring studies [34], [35] support this application context, while the present prototype extends it with access verification, token logic, protection, and separated notification roles.

The evidence remains bounded by a laboratory prototype with two loads and generally stable connectivity. The study does not provide a calibrated reference dataset, repeated-sample statistics, long-term drift measurements, diverse appliance profiles, multi-user trials, adversarial security testing, or interoperability tests with Matter or Zigbee. The coverage count in Table 5 is an implementation checklist, not a standardized usability or quality metric. These limitations identify the specific evidence required for field validation without extending the claims beyond the reported results.

4. CONCLUSION

The study demonstrates laboratory-scale feasibility for coordinating continuous monitoring, two-load control, RFID authorization, token state, local protection, and event-specific communication in one ESP32-based prototype. Wi-Fi initialized within 2-5 s, WhatsApp messages were observed within 1-2 s, line voltage was 216-221 V across the six reported load scenarios, and the controller executed the expected response in each scenario, including disconnection above 3.5 A. The broader implication is that affordable household systems can separate routine supervision from urgent escalation while keeping both tied to the same control decision. Deployment evidence must still establish measurement accuracy, security, interoperability, and reliability under real residential and variable-network conditions.

ACKNOWLEDGMENTS

The authors used OpenAI ChatGPT Work (Codex, GPT-5 series; accessed 23 August 2026) solely to assist with language editing, organization, consistency checking, and implementation of reviewer-requested formatting during revision. All technical content, data, analyses, interpretations, figures, and final wording were reviewed and approved by the authors. No generative AI was used to create research data or alter the scientific content of the figures.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ryan Fikri	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Agariadne Dwinggo Samala		✓				✓	✓	✓	✓	✓	✓	✓		
Gustia Fernando	✓		✓				✓	✓	✓					
Soha Rawas				✓	✓					✓				

C : **C**onceptualizationM : **M**ethodologySo : **S**oftwareVa : **V**alidationFo : **F**ormal analysisI : **I**nterpretationR : **R**esourcesD : **D**ata CurationO : **O**riginal DraftE : **E**ditingVi : **V**isualizationSu : **S**upervisionP : **P**roject administrationFu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, Ryan Fikri, upon reasonable request.

REFERENCES

- [1] K. Malek *et al.*, "Design and implementation of sustainable solar energy harvesting for low-cost remote sensors equipped with real-time monitoring systems," *Journal of Infrastructure Intelligence and Resilience*, vol. 2, no. 3, pp. 1–17, Sep. 2023, doi: 10.1016/j.jintel.2023.100051.
- [2] M. S. Hossain and I. A. Chowdhury, "DATAEMS: Design and development of a data analysis-based energy monitoring system," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 6, pp. 1–11, Dec. 2023, doi: 10.1016/j.prime.2023.100387.
- [3] M. K. Gupta *et al.*, "Real-time monitoring and measurement of energy characteristics in sustainable machining of titanium alloys," *Measurement*, vol. 224, pp. 1–18, Jan. 2024, doi: 10.1016/j.measurement.2023.113937.
- [4] F. Chen and G. Fang, "Harnessing digital twin and IoT for real-time monitoring, diagnostics, and error correction in domestic solar energy storage," *Energy Reports*, vol. 11, pp. 3614–3623, Jun. 2024, doi: 10.1016/j.egyr.2024.03.024.
- [5] Z. Ye *et al.*, "IoT-enhanced smart road infrastructure systems for comprehensive real-time monitoring," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 235–249, 2024, doi: 10.1016/j.iotcps.2024.01.002.
- [6] S. Khemakhem and L. Krichen, "A comprehensive survey on an IoT-based smart public street lighting system application for smart cities," *Franklin Open*, vol. 8, pp. 1–12, Sep. 2024, doi: 10.1016/j.fraope.2024.100142.
- [7] S. Dorahaki, M. MollahassaniPour, and M. Rashidinejad, "Optimizing energy payment, user satisfaction, and self-sufficiency in flexibility-constrained smart home energy management: A multi-objective optimization approach," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 6, pp. 1–12, Dec. 2023, doi: 10.1016/j.prime.2023.100385.
- [8] T. L. Narayana *et al.*, "Advances in real time smart monitoring of environmental parameters using IoT and sensors," *Heliyon*, vol. 10, no. 7, pp. 1–22, Apr. 2024, doi: 10.1016/j.heliyon.2024.e28195.
- [9] H. J. El-Khozondar *et al.*, "A smart energy monitoring system using ESP32 microcontroller," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 9, pp. 1–10, Sep. 2024, doi: 10.1016/j.prime.2024.100666.
- [10] M. Esposito, A. Belli, L. Palma, and P. Pierleoni, "Design and implementation of a framework for smart home automation based on cellular IoT, MQTT, and serverless functions," *Sensors*, vol. 23, no. 9, pp. 1–16, May 2023, doi: 10.3390/s23094459.
- [11] P. M. Rao and B. D. Deebak, "A comprehensive survey on authentication and secure key management in Internet of Things: Challenges, countermeasures, and future directions," *Ad Hoc Networks*, vol. 146, Jul. 2023, doi: 10.1016/j.adhoc.2023.103159.
- [12] Sunardi, A. Yudhana, and Furizal, "Tsukamoto fuzzy inference system on Internet of Things-based for room temperature and humidity control," *IEEE Access*, vol. 11, pp. 6209–6227, 2023, doi: 10.1109/ACCESS.2023.3236183.
- [13] A. A. Zakri, R. A. R. Q. Y. Putri, S. Romadoni, and Y. Hasneli, "IoT-based flex sensor gloves for immobility patients: A prototype," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 14, no. 3, pp. 920–927, Jun. 2024, doi: 10.18517/ijaseit.14.3.19514.
- [14] R. E. Putri, N. U. Lestari, Ifmalinda, F. Arlius, I. Putri, and A. Hasan, "Monitoring and controlling system of smart mini greenhouse based on Internet of Things (IoT) for spinach plant (*Amaranthus sp.*)," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 14, no. 1, pp. 131–136, Feb. 2024, doi: 10.18517/ijaseit.14.1.18408.
- [15] E. S. Kaseng, M. A. Syifani, and A. M. A. Mukhlis, "Development and working test of microcontroller-based automatic seedling tools for hydroponic systems," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 14, no. 2, pp. 738–748, Apr. 2024, doi: 10.18517/ijaseit.14.2.19862.
- [16] P. Anuradha, K. Vasanth, G. Renuka, and A. R. Rao, "IoT based enabling home automation system for individuals with diverse disabilities," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 6, pp. 1–5, Dec. 2023, doi: 10.1016/j.prime.2023.100366.
- [17] M. Umair, M. A. Cheema, B. Afzal, and G. Shah, "Energy management of smart homes over fog-based IoT architecture," *Sustainable Computing: Informatics and Systems*, vol. 39, Sep. 2023, doi: 10.1016/j.suscom.2023.100898.
- [18] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, "Investigating smart home security: Is blockchain the answer?," *IEEE Access*, vol. 8, pp. 117802–117816, 2020, doi: 10.1109/ACCESS.2020.3004662.

- [19] S. Gupta *et al.*, "Smart agriculture using IoT for automated irrigation, water and energy efficiency," *Smart Agricultural Technology*, vol. 12, Dec. 2025, doi: 10.1016/j.atech.2025.101081.
- [20] A. Jain, A. Bhola, S. Upadhyay, A. Singh, D. Kumar, and A. Jain, "Secure and smart trolley shopping system based on IoT module," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, Dec. 2022, pp. 2243–2247, doi: 10.1109/IC3I56241.2022.10073159.
- [21] M. R. Islam, K. Oliullah, M. M. Kabir, M. Alom, and M. F. Mridha, "Machine learning enabled IoT system for soil nutrients monitoring and crop recommendation," *Journal of Agriculture and Food Research*, vol. 14, Dec. 2023, doi: 10.1016/j.jafr.2023.100880.
- [22] A. Morchid, R. Jebabra, H. M. Khalid, R. El Alami, H. Qjidaa, and M. O. Jamil, "IoT-based smart irrigation management system to enhance agricultural water security using embedded systems, telemetry data, and cloud computing," *Results in Engineering*, vol. 23, Sep. 2024, doi: 10.1016/j.rineng.2024.102829.
- [23] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "IoT connectivity technologies and applications: A survey," *IEEE Access*, vol. 8, pp. 67646–67673, 2020, doi: 10.1109/ACCESS.2020.2985932.
- [24] O. Ali, M. K. Ishak, M. K. L. Bhatti, I. Khan, and K.-I. Kim, "A comprehensive review of Internet of Things: Technology stack, middlewares, and fog/edge computing interface," *Sensors*, vol. 22, no. 3, pp. 1–43, Jan. 2022, doi: 10.3390/s22030995.
- [25] Y. Y. F. Panduman, N. Funabiki, P. Puspitaningayu, M. Kuribayashi, S. Sukaridhoto, and W.-C. Kao, "Design and implementation of SEMAR IoT server platform with applications," *Sensors*, vol. 22, no. 17, pp. 1–28, Aug. 2022, doi: 10.3390/s22176436.
- [26] P. Chiradeja and S. Yoomak, "Development of public lighting system with smart lighting control systems and internet of thing (IoT) technologies for smart city," *Energy Reports*, vol. 10, pp. 3355–3372, Nov. 2023, doi: 10.1016/j.egyr.2023.10.027.
- [27] R. M. Ramli and W. A. Jabbar, "Design and implementation of solar-powered with IoT-Enabled portable irrigation system," *Internet of Things and Cyber-Physical Systems*, vol. 2, pp. 212–225, 2022, doi: 10.1016/j.iotcps.2022.12.002.
- [28] F. Ahmed, M. H. I. Bijoy, H. R. Hemal, and S. R. H. Noori, "Smart aquaculture analytics: Enhancing shrimp farming in Bangladesh through real-time IoT monitoring and predictive machine learning analysis," *Heliyon*, vol. 10, no. 17, pp. 1–19, Sep. 2024, doi: 10.1016/j.heliyon.2024.e37330.
- [29] S. W. Nourillean and M. D. Hassib, "IoT-based MANET performance improvement against jamming attackers in different mobile applications," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, pp. 1–11, Jun. 2024, doi: 10.1016/j.prime.2024.100615.
- [30] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review," *Sensors*, vol. 23, no. 2, pp. 1–43, Jan. 2023, doi: 10.3390/s23020788.
- [31] N. Singh, R. Buyya, and H. Kim, "Securing cloud-based Internet of Things: Challenges and mitigations," *Sensors*, vol. 25, no. 1, pp. 1–45, Dec. 2024, doi: 10.3390/s25010079.
- [32] N. Ramachandra and R. Natarajan, "State-of-the-art and real-time implementation of an IoT-based home energy management system for a cluster of dwellings," *Heliyon*, vol. 10, no. 16, pp. 1–22, Aug. 2024, doi: 10.1016/j.heliyon.2024.e35887.
- [33] M. Umer *et al.*, "IoT based smart home automation using blockchain and deep learning models," *PeerJ Computer Science*, vol. 9, May 2023, doi: 10.7717/peerj-cs.1332.
- [34] R. Fitriyan and S. Syafii, "Development design of an IoT-based smart home monitoring system with security features," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 2, pp. 788–794, May 2024, doi: 10.11591/ijeecs.v34.i2.pp788-794.
- [35] W. Agustiarini *et al.*, "Real-time IoT-based energy power consumption monitoring system for smart homes," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 15, no. 5, pp. 1407–1412, Oct. 2025, doi: 10.18517/ijaseit.15.5.20918.

BIOGRAPHIES OF AUTHORS



Ryan Fikri    earned his Master's degree in Engineering from Institut Teknologi Bandung (ITB), where he specialized in high altitude platform station (HAPS) research. He is a full-time lecturer actively engaged in studies on electronics, telecommunications, and the internet of things. He has contributed to national spectrum management under the Ministry of Communication and Informatics, supporting regulatory initiatives to optimize frequency usage in Indonesia. His expertise in telecommunications was further recognized through his involvement in the Indonesia 5G taskforce, reflecting his commitment to advancing next-generation network technologies in the country. He can be contacted at email: ryanfikri@ft.unp.ac.id.



Agariadne Dwinggo Samala    is an Associate Professor at the Faculty of Engineering, Universitas Negeri Padang (UNP), Indonesia, and an affiliated tutor at Universitas Terbuka. He completed his Ph.D. in Technology and Vocational Education at UNP, focusing on the integration of technology in education. His research interests include technology-enhanced learning, educational technology, bibliometrics, systematic reviews, immersive learning, and emerging educational technologies. He can be contacted at email: agariadne@ft.unp.ac.id.



Gustia Fernando    is an undergraduate student in the Electronics Engineering Education Study Program, Faculty of Engineering, Universitas Negeri Padang (UNP), Indonesia. His academic interests focus on the internet of things and artificial intelligence. He has served as Head of the Achievement and Academic Division in the Electronics Engineering Student Association and has participated in research collaborations and the 2025 Student Creativity Program (PKM). He is actively involved in developing internet of thing-based prototypes and exploring emerging educational and industrial technologies. He can be contacted at email: gustiafernando08@gmail.com.



Soha Rawas    holds a Ph.D. in Mathematics and Computer Science from Beirut Arab University (2019). Her research spans artificial intelligence, deep learning, IoMT, cloud computing, medical image processing, secure intelligent systems, and AI in education, with applications across healthcare, learning technologies, and smart systems. She is a faculty member in the Department of Mathematics and Computer Science, Faculty of Science at BAU, and serves as the Director of the Continuing Education Center (CEC), leading strategic development, digital transformation, and innovative training programs across diverse professional fields. She can be contacted at email: soha.rawas2@bau.edu.lb.