



Design and Performance Analysis of IoT-Based Smart Home Automation Systems

Pyarali Jadoonwala

Department of Electrical and Computer Engineering, Peninsula Institute of Engineering Studies, Malaysia
pyarali.jadoonwala@pies-my.edu

Peer Review Information

Submission: 03 Feb 2019
Revision: 17 March 2019
Acceptance: 07 April 2019

Keywords

Internet of Things, Smart Home, Home Automation, MQTT, Energy Management

Abstract

The Internet of Things (IoT) has transformed home automation from isolated electronic control into a connected environment in which sensors, controllers, cloud services, and user interfaces cooperate in real time. This methodology paper presents the design and performance analysis of a low-cost IoT-based smart home automation architecture intended for appliance control, environmental monitoring, security notification, and basic energy management. The proposed design uses sensor nodes connected to a NodeMCU-class controller, Wi-Fi connectivity, MQTT-style publish/subscribe messaging, relay-based actuation, and a mobile/web dashboard. The methodology combines architectural design with a simulation-based performance evaluation so that latency, command success rate, packet loss, and household energy use can be examined without claiming an unperformed physical experiment. Four communication conditions are modeled over 300 control transactions per condition, while a 24-hour appliance-load model is used to estimate the effect of occupancy-aware automation. The generated results indicate that local and sensor-triggered control can provide sub-0.2 s average responses, whereas cloud and congested links introduce higher delay. The energy model produces an estimated reduction of about 14% compared with a non-automated operating schedule. The study concludes that a gateway-centered IoT architecture can provide responsive and energy-aware home automation, while security, interoperability, and network dependence remain important design constraints.

Introduction

A smart home integrates sensing, communication, computation, and actuation to provide automated or remotely controlled domestic services. In an IoT implementation, ordinary appliances and environmental sensors are converted into network-addressable devices that can exchange data, receive commands, and coordinate actions through a gateway or cloud platform. Earlier smart-home solutions often depended on isolated proprietary systems, whereas IoT architectures emphasize Internet connectivity, heterogeneous device integration,

mobile access, and data-driven services. Risteska Stojkoska and Trivodaliev (2017) described this transition as a movement toward holistic IoT frameworks that combine smart objects, communication protocols, processing resources, and management services. A systematic review by Alaa et al. (2017) similarly showed that smart-home research had expanded from simple remote switching to applications involving security, energy optimization, healthcare, and context-aware control.

The practical value of IoT-based automation lies in the ability to monitor household conditions

continuously and respond with limited user intervention. Temperature, humidity, motion, smoke, gas, light, and door sensors can generate events, while relays and smart plugs can control lights, fans, air conditioners, pumps, and other appliances. Mocrii et al. (2018) observed that a modern smart home requires a coordinated architecture spanning sensors, software, communication technologies, privacy mechanisms, and system-management functions. Wireless connectivity is especially important because installation cost and physical flexibility strongly affect domestic adoption. Wi-Fi is attractive for low-cost prototypes because it is widely available and offers direct IP connectivity, while protocols such as ZigBee can provide lower-power sensing networks. Froiz-Míguez et al. (2018) demonstrated that MQTT and gateway/fog processing can support scalable home automation and can reduce response time by performing time-sensitive work near the devices rather than exclusively in the cloud. Low-cost embedded platforms have enabled practical smart-home systems using Arduino, NodeMCU, cloud services, sensors, relays, and mobile interfaces (Jabbar et al., 2018, 2019). These studies show that affordable components can provide effective monitoring and appliance control, although performance depends on network reliability and communication design. Elsts et al. (2017) emphasized robustness and long-term reliability in residential sensing. Security and privacy are also critical, with gateway-based architectures proposed for resource-constrained devices (Lin & Bergmann, 2016). Hoque and Davidson (2019) demonstrated security-oriented integration, while Lashkari et al. (2019), Filho et al. (2019), and You et al. (2019) highlighted energy efficiency, intelligent control, and secure communication.

Accordingly, this paper proposes a compact smart-home architecture and a reproducible methodology for evaluating its performance. The study focuses on four questions: (1) how should sensing, control, messaging, cloud access, and user interfaces be organized; (2) what response times can be expected under local, automated, remote, and congested communication conditions; (3) how reliably can commands be delivered; and (4) what energy-saving potential can be obtained from simple occupancy-aware scheduling. The objective is not to claim a physical prototype that was not built, but to provide a transparent methodology and simulation-based analysis that can be implemented later on real hardware.

Literature Review

Research up to 2019 shows three recurring design themes: layered architecture, lightweight communication, and application-specific optimization. Risteska Stojkoska and Trivodaliev (2017) proposed a holistic view in which sensing devices, local networks, processing services, and cloud resources cooperate as a complete smart-home management system. Alaa et al. (2017) organized the literature into application, framework, and implementation categories and identified interoperability, security, acceptance, and efficient service delivery as persistent open problems. Mocrii et al. (2018) extended this architectural discussion by reviewing smart-home software, communication mechanisms, privacy, and security; their analysis is especially relevant because home automation is not only an electronics problem but also a systems-integration problem.

Communication choice directly affects responsiveness and scalability. Froiz-Míguez et al. (2018) combined MQTT with ZigBee-Wi-Fi sensor nodes and fog services, showing the suitability of publish/subscribe communication and edge processing for home automation. Jabbar et al. (2018) emphasized a low-cost Wi-Fi implementation in which environmental sensors, relays, and a mobile application formed a straightforward end-to-end control loop. These approaches support the use of a NodeMCU/Wi-Fi gateway in the present design because it reduces hardware complexity while retaining Internet connectivity and compatibility with lightweight messaging.

Reliability and security are equally important. Elsts et al. (2017), based on the SPHERE residential sensing platform, reported practical difficulties associated with embedded resource limits, heterogeneous devices, robust networking, and long-duration operation. Lin and Bergmann (2016) focused on security and privacy, arguing that a smart-home gateway can mediate protection for devices that cannot implement heavyweight security mechanisms themselves. Hoque and Davidson (2019) showed a gateway and web-service design for home security that links sensors and microcontrollers to a mobile user interface. These works motivate the use of authenticated application access, segmented local control, and a gateway responsible for forwarding data to external services.

By 2019, research also increasingly connected home automation with energy management. Lashkari et al. (2019) reviewed sensor-driven energy monitoring, data management, and intelligent control, while Filho et al. (2019) examined the combination of wireless

sensor/actuator networks and computational intelligence for energy-efficient homes. Jabbar et al. (2019) demonstrated an integrated IoT home platform capable of sensing, appliance control, safety functions, and energy-aware operation. You et al. (2019) concluded that IoT smart homes require the combined treatment of wireless

performance, security, energy management, artificial intelligence, and service quality. The gap addressed in the present methodology is therefore a compact, transparent evaluation framework that simultaneously measures communication responsiveness, delivery reliability, and simple energy-saving behavior.

Table 1. Representative IoT smart-home studies used to shape the methodology.

Study	Main focus	Technology contribution /	Methodological implication
Lin & Bergmann (2016)	Privacy/security	Gateway-oriented protection	Centralize policy and access control
Elsts et al. (2017)	Residential IoT reliability	Low-power heterogeneous sensing	Evaluate robustness and delivery
Froiz-Míguez et al. (2018)	MQTT/fog automation	ZigBee-Wi-Fi + MQTT	Measure local vs remote latency
Jabbar et al. (2018)	Low-cost automation	Arduino + Wi-Fi + mobile app	Use simple IP-based control loop
Hoque & Davidson (2019)	Home security	Sensors + gateway + web/mobile	Include alerts and secure access
Jabbar et al. (2019)	Integrated smart home	NodeMCU, cloud, relays, sensors	Combine monitoring and appliance control

Methodology

The methodology follows four sequential stages: system architecture design, control-rule definition, communication simulation, and energy-use estimation. This organization makes the analysis reproducible and separates architectural decisions from performance assumptions.

1. System Architecture and Components

The proposed system is organized into five functional blocks: (i) sensors, (ii) edge controller, (iii) Wi-Fi/MQTT messaging, (iv) cloud/dashboard services, and (v) user application. Temperature/humidity, motion, gas/smoke, and door sensors represent the sensing layer. A NodeMCU-class ESP8266/ESP32

controller is selected as the edge device because it integrates a microcontroller with Wi-Fi connectivity and can host lightweight control logic. Relay channels connect the controller to representative appliances. The controller reads sensors at fixed intervals and publishes state changes to an MQTT broker or equivalent message service. User commands travel in the reverse direction and are verified before actuation. Local rules are allowed to execute even if the Internet link is unavailable; for example, motion and illumination conditions can switch lights, while gas/smoke detection can force an alarm output. This local-first structure follows the latency advantages observed for edge/fog processing by Froiz-Míguez et al. (2018).

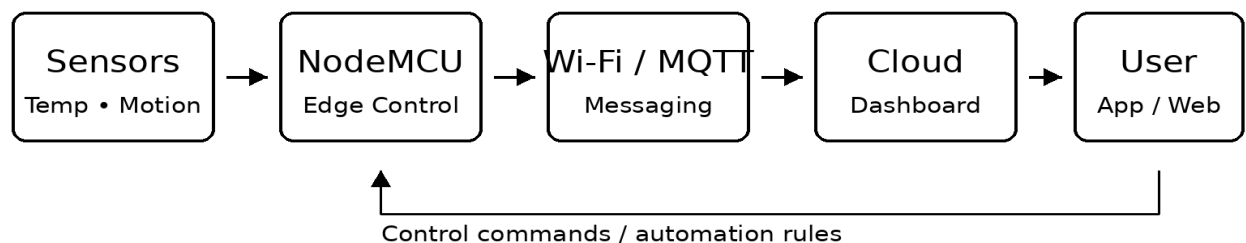


Figure 1. Proposed IoT-based smart home automation architecture.

2. Communication and Control Logic

MQTT-style publish/subscribe communication is used because it decouples sensor publishers from control subscribers and can operate efficiently on constrained devices. Example topics include home/ room1/ temperature, home/ security/ motion, and home/appliance/light1/set. Each

message contains a timestamp, device identifier, measured value or command, and a simple status field. For a real deployment, transport encryption, authenticated broker access, unique device credentials, and restricted topic permissions should be applied in line with the security concerns identified by Lin and

Bergmann (2016) and You et al. (2019). Local automation rules are intentionally simple: if motion is absent beyond a configured timeout, unnecessary lighting is switched off; if indoor temperature exceeds a threshold and occupancy is present, fan/air-conditioning control is enabled; if smoke/gas is detected, an alarm and mobile notification are generated. Manual user commands override non-safety automation for a limited period.

3. Performance Evaluation Procedure

Because no physical hardware experiment is claimed in this paper, performance is evaluated through a controlled Monte Carlo communication model. Four operating conditions are considered: local app control on the home Wi-Fi network, sensor-triggered local automation, remote cloud control under normal Internet conditions, and remote control under congestion. For each condition, 300 transactions are generated. Latency is sampled from a truncated normal distribution whose mean and spread reflect the expected ordering reported in prior edge/cloud smart-home work: local processing is modeled as the fastest, cloud access is slower, and congestion adds further delay. Command delivery is represented by a Bernoulli success process. The primary metrics are mean end-to-end response

time, 95th-percentile latency, command success rate, and packet/transaction loss. The fixed random seed (42) makes the reported simulation reproducible. These results should be treated as design-stage estimates; a future hardware prototype should repeat the same procedure with measured timestamps.

4. Energy-Use Estimation

A 24-hour appliance-load model is used to estimate energy-management potential. The baseline schedule assumes 1.20 kWh/day for lighting, 1.28 kWh/day for fans, 7.20 kWh/day for air conditioning, 0.75 kWh/day for a water pump, and 2.88 kWh/day for standby loads, totaling 13.31 kWh/day. The automated schedule reduces unnecessary lighting duration, fan operating time, air-conditioning runtime, and standby consumption through occupancy rules and smart switching, while the water-pump demand is left unchanged. The resulting modeled load is 11.44 kWh/day. The percentage saving is calculated as $(E_{\text{baseline}} - E_{\text{smart}})/E_{\text{baseline}} \times 100$. This simplified method follows the energy-management motivation emphasized by Lashkari et al. (2019) and Filho et al. (2019), but it is not intended to replace building-specific thermal or tariff models.

Table 2. Simulation and energy-model parameters.

Parameter	Value	Purpose
Transactions per communication condition	300	Stable comparative latency/reliability estimate
Random seed	42	Reproducibility
Control paths	Local, sensor-triggered, remote, congested	Compare network dependence
Evaluation metrics	Mean latency, p95 latency, success, loss	Responsiveness and reliability
Baseline daily energy	13.31 kWh	Reference non-automated schedule
Automated daily energy	11.44 kWh	Occupancy-aware schedule

Results

The simulation produces the expected separation between local and Internet-dependent control. Sensor-triggered automation is the fastest path because the decision is executed at the edge without waiting for a remote user interface. Local app control remains well below 0.2 s on average, whereas remote cloud control is approximately three times slower. Under congestion, both

average and tail latency increase substantially and the delivery rate declines. This behavior is consistent with the design rationale for local/fog processing discussed by Froiz-Míguez et al. (2018). The values in Table 3 are generated by the stated simulation model and should therefore be interpreted as reproducible design-stage estimates rather than measurements from a completed physical installation.

Table 3. Simulated communication performance of the proposed architecture.

Condition	Mean latency (ms)	95th percentile (ms)	Success (%)	Loss (%)
Local app control	109.0	148.0	99.0	1.0
Sensor-triggered automation	76.8	108.1	99.3	0.7

Remote cloud control	295.9	417.4	98.3	1.7
Congested remote control	447.4	625.3	95.3	4.7

The energy model gives a baseline demand of 13.31 kWh/day and an automated demand of 11.44 kWh/day, corresponding to an estimated saving of 14.0%. The largest absolute reduction comes from air-conditioning runtime, followed by standby loads and lighting. This result should not be generalized as a universal household saving because actual performance depends on occupancy, climate, appliance efficiency, tariff structure, and user behavior. Nevertheless, it demonstrates how a smart-home controller can convert sensing information into measurable operational changes rather than merely offering remote switching. This is aligned with the broader energy-management direction reviewed by Lashkari et al. (2019) and Filho et al. (2019). From a design perspective, the combined results suggest three priorities. First, safety and time-sensitive automation should remain executable locally so that the system is not dependent on Internet round trips. Second, cloud connectivity is useful for remote monitoring, historical storage, and notifications but should not be the only control path. Third, the communication layer should expose performance and health indicators so that packet loss, unreachable nodes, and abnormal delay can be detected. The integrated sensor/cloud model is consistent with the practical implementations of Hoque and Davidson (2019) and Jabbar et al. (2019), while the architectural emphasis on interoperability and heterogeneous services follows the challenges identified by Mocrii et al. (2018).

Conclusion and Discussion

This methodology paper presented the design and performance analysis of an IoT-based smart home automation system using a gateway-centered architecture, Wi-Fi connectivity, MQTT-style messaging, sensor-driven rules, relay actuation, cloud monitoring, and mobile/web access. The design reflects the evolution of smart-home research toward integrated IoT platforms in which sensing, communication, computation, security, and energy management must be considered together (Risteska Stojkoska & Trivodaliev, 2017; Alaa et al., 2017). The use of a NodeMCU-class edge controller and local automation rules provides a practical low-cost implementation path similar to the architectures demonstrated by Jabbar et al. (2018, 2019). The simulation-based performance analysis shows why control-path placement matters. Sensor-triggered and local user commands achieve the lowest modeled response times, while cloud routing adds delay and congestion increases both

latency and transaction loss. These findings support the use of edge/fog processing for time-sensitive home functions, consistent with Froiz-Míguez et al. (2018). The modeled 14% energy reduction also illustrates the potential value of occupancy-aware control and standby-load management, although actual savings would need to be validated with instrumented household data. Energy management should therefore be treated as a context-dependent optimization problem rather than a guaranteed fixed percentage (Lashkari et al., 2019; Filho et al., 2019). Several limitations remain. The analysis is simulation-based, not a hardware benchmark; wireless interference, router implementation, MQTT broker loading, sensor noise, and actuator switching delays are represented only indirectly. The energy model does not simulate building thermal dynamics. In addition, a real deployment must protect user data and physical control functions through authentication, encryption, topic-level authorization, secure software updates, and fault-tolerant local behavior, as emphasized by Lin and Bergmann (2016). Long-duration operation should also consider device failure, battery constraints, and software maintainability, issues demonstrated by the SPHERE experience (Elsts et al., 2017). Future work should implement the architecture on ESP32/NodeMCU hardware, collect timestamped MQTT traffic under different Wi-Fi loads, measure appliance energy with calibrated smart meters, and compare edge-only, cloud-only, and hybrid control. Additional work can include anomaly detection, voice interfaces, machine learning for activity prediction, and interoperable standards. Overall, the proposed methodology provides a concise and reproducible starting point for evaluating IoT smart-home systems in terms of responsiveness, reliability, energy awareness, and deployability, while remaining consistent with the key smart-home research directions summarized by You et al. (2019).

References

- Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, 97, 48–65. <https://doi.org/10.1016/j.jnca.2017.08.017>
- Elsts, A., Oikonomou, G., Fafoutis, X., & Piechocki, R. (2017). Internet of Things for smart homes: Lessons learned from the SPHERE case study.

2017 Global Internet of Things Summit (GloTS).
<https://doi.org/10.1109/GIOTS.2017.8016226>

Filho, G. P. R., Villas, L. A., Gonçalves, V. P., Pessin, G., Loureiro, A. A. F., & Ueyama, J. (2019). Energy-efficient smart home systems: Infrastructure and decision-making process. *Internet of Things*, 5, 153–167.
<https://doi.org/10.1016/j.iot.2018.12.004>

Froiz-Míguez, I., Fernández-Caramés, T. M., Fraga-Lamas, P., & Castedo, L. (2018). Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes. *Sensors*, 18(8), 2660.
<https://doi.org/10.3390/s18082660>

Hoque, M. A., & Davidson, C. (2019). Design and implementation of an IoT-based smart home security system. *International Journal of Networked and Distributed Computing*, 7, 85–92.
<https://doi.org/10.2991/ijndc.k.190326.004>

Jabbar, W. A., Alsibai, M. H., Amran, N. S. S., & Mahayadin, S. K. (2018). Design and implementation of IoT-based automation system for smart home. 2018 International Symposium on Networks, Computers and Communications (ISNCC).
<https://doi.org/10.1109/ISNCC.2018.8531006>

Jabbar, W. A., Kian, T. K., Ramli, R. M., Zubir, S. N., Zamrizaman, N. S. M., Balfaiah, M., Shepelev, V., &

Alharbi, S. (2019). Design and fabrication of smart home with Internet of Things enabled automation system. *IEEE Access*, 7, 144059–144074.
<https://doi.org/10.1109/ACCESS.2019.2942846>

Lashkari, B., Chen, Y., & Musilek, P. (2019). Energy management for smart homes—State of the art. *Applied Sciences*, 9(17), 3459.
<https://doi.org/10.3390/app9173459>

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information*, 7(3), 44.
<https://doi.org/10.3390/info7030044>

Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, 1–2, 81–98.
<https://doi.org/10.1016/j.iot.2018.08.009>

Risteska Stojkoska, B. L., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140, 1454–1464.
<https://doi.org/10.1016/j.jclepro.2016.10.006>

You, I., Pau, G., Salerno, V. M., & Sharma, V. (2019). Special issue “Internet of Things for Smart Homes”. *Sensors*, 19(19), 4173.
<https://doi.org/10.3390/s19194173>