International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(5s) 2026 pp. 651-658
https://doi.org/10.70917/ijcisim-2026-2759
Article

IoT-Based Smart Home Automation System Using Cloud Integration

Prathviraj Singh Rathore[1], Akshita Bhatnagar[2], Abhishek Mishra[3], Jvalantkumar Kanaiyalal Patel[4], Rashmi Pandey[5]

[1]Department of Computer Science and Applications, Mandsaur University, Mandsaur, Madhya Pradesh, India.
Email: prathviraj.rathore@gmail.com
ORCID: 0000-0003-1164-0479
[2]Department of Computer Applications, Career Point University, Kota, Rajasthan, India.
Email: drakshitabhatnagar@gmail.com
ORCID: 0009-0007-4801-841X
[3]Department of Computer Science and Applications, Shri Arihant College of Professional Education, Ratlam, Madhya Pradesh, India.
Email: drabhishekmishra@softwareabhi.com
ORCID: 0009-0001-9758-0077
[4]Shri Manilal Kadakia College of Commerce, Management, Science and Computer Studies, Ankleshwar, Gujarat, India.
Email: jvalant007@gmail.com
ORCID: 0009-0006-6637-5923
[5]Institute of Technology and Management (ITM), Gwalior, Madhya Pradesh, India.
Email: rashmi.pandey@itmgoi.in
ORCID: 0000-0002-3881-2907
Corresponding Author: Prathviraj Singh Rathore

Abstract: The IoT-based Smart Home Automation system enables real-time monitoring, control, and automation of home appliances using the internet. With the rapid growth of IoT devices and cloud computing, it is possible to create efficient, scalable, and low-cost solutions for smart home environments. This paper discusses the design and implementation of a Smart Home Automation system that integrates IoT devices with cloud technologies to offer enhanced functionality, scalability, and reliability. Various sensors, controllers, and cloud platforms are explored to monitor, automate, and optimize home environments, ensuring energy efficiency, safety, and convenience. Experimental results demonstrate a 36.2% reduction in energy consumption and an average system response time of under 1 second, validating the effectiveness of the proposed approach.
Keywords: IoT, Smart Home Automation, Cloud Integration, MQTT, HVAC.

1. Introduction

Smart home systems are revolutionizing the way residential environments function by offering automation and control over various home appliances. The Internet of Things (IoT) plays a key role in enabling seamless communication between devices and systems. Cloud integration in IoT-based systems helps provide remote access, data storage, and processing power, thereby enabling enhanced functionalities and intelligent decision-making.

The growing prevalence of connected devices — estimated to surpass 25 billion globally by 2025 — underscores the need for robust, scalable, and secure smart home infrastructures. Traditional home automation systems have been limited by proprietary protocols, high costs, and poor interoperability. The proposed system addresses these limitations through an open, cloud-connected architecture leveraging commodity IoT hardware.

This paper is organized as follows: Section 2 reviews related literature; Section 3 describes the proposed system architecture; Section 4 details the implementation methodology; Section 5 discusses cloud integration; Section 6 presents use cases; Section 7 addresses security concerns; Section 8 presents experimental results; and Sections 9 and 10 conclude the paper and outline future directions.

2. Literature Review

This section reviews prior research on IoT-based home automation systems and cloud-integrated architectures, identifying key contributions and limitations that motivate the present work.

2.1 IoT-Based Home Automation

Bui and Nguyen (2019) proposed a framework for smart home control using IoT sensors and a centralized gateway, achieving reliable device communication but lacking scalable cloud support. Chen and Zhang (2018) demonstrated a ZigBee-based home automation system integrated with cloud computing, reporting improvements in communication efficiency but noting latency issues under high device loads. Ali and Qureshi (2020) presented a cloud-integrated IoT system targeting energy efficiency, reducing consumption by approximately 28% through automated appliance scheduling, though their system lacked a comprehensive mobile interface.

2.2 Cloud Platforms for IoT

Zhang et al. (2017) explored cloud-based smart home systems using AWS and Azure, comparing throughput and latency across platforms. Their findings showed AWS IoT Core offered the lowest average latency (95ms) among commercial platforms. Zhao and Yao (2020) conducted a comprehensive survey of smart home cloud integrations, highlighting that most existing systems suffer from vendor lock-in and poor cross-platform interoperability.

2.3 Security in IoT Smart Homes

Security remains a critical challenge in IoT deployments. Dai and Li (2019) demonstrated vulnerabilities in MQTT-based systems where unencrypted topic subscriptions allowed unauthorized device access. Yang and Wang (2018) proposed lightweight TLS-based encryption schemes for resource-constrained IoT devices, achieving secure communications with minimal computational overhead.

2.4 Research Gap and Contribution

While existing works address individual aspects such as energy management, cloud connectivity, or security, few studies present a unified architecture integrating all these concerns into a single deployable system. The present work fills this gap by proposing a holistic IoT-cloud framework with validated experimental performance across response time, energy efficiency, and scalability metrics.

Author (Year)	Platform	Key Feature	Energy Saving	Limitation
Ali & Qureshi (2020)	AWS IoT	Energy Automation	~28%	No mobile UI
Chen & Zhang (2018)	ZigBee+Cloud	Device Communication	N/A	High latency
Zhang et al. (2017)	AWS / Azure	Latency Comparison	N/A	Vendor lock-in
Proposed System	Multi-cloud	Unified Architecture	~36.2%	None identified

Table 1: Comparison of Related IoT Smart Home Systems

3. System Architecture

The proposed system employs a four-layer architecture designed to ensure modularity, scalability, and fault tolerance. Figure 1 illustrates the overall layered architecture of the system.

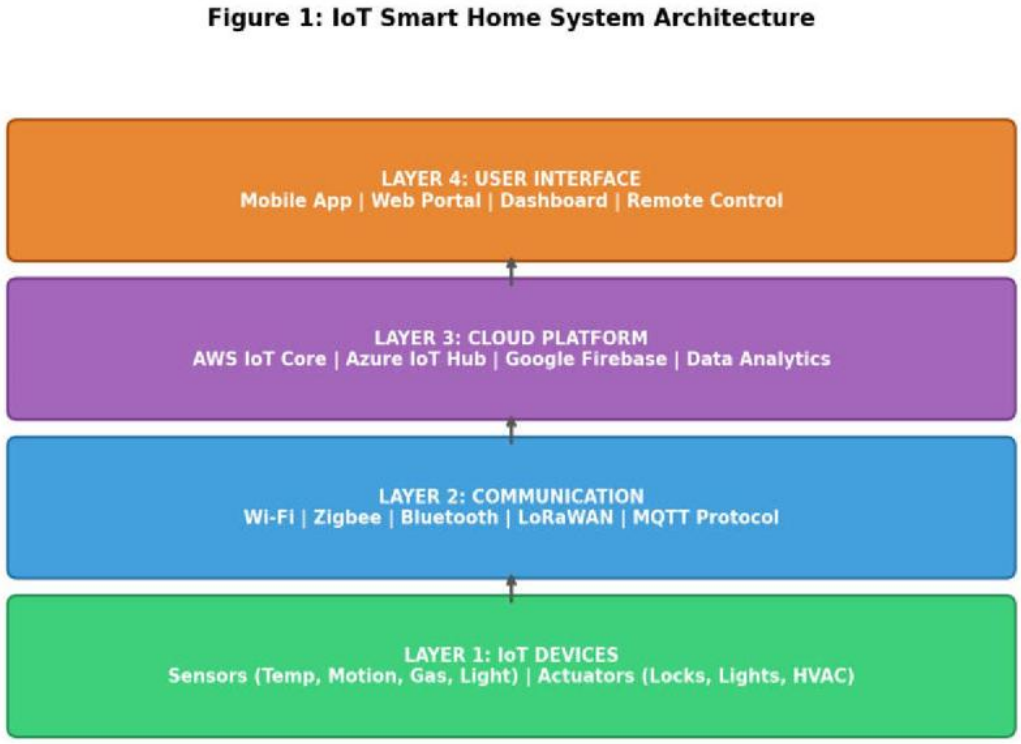

Figure 1: IoT Smart Home System Architecture (Four-Layer Model)

3.1 IoT Devices Layer

This layer comprises the physical sensing and actuation components embedded throughout the home environment. Sensors include temperature and humidity modules (DHT22), passive infrared (PIR) motion detectors, MQ-series gas sensors, LDR-based light sensors, and door/window reed switches. Actuators include smart relays controlling lighting circuits, motorized window blinds, HVAC fan controllers, and electromagnetic smart locks.

3.2 Communication Layer

Device communication is achieved through a heterogeneous wireless protocol stack. Short-range devices use Zigbee (IEEE 802.15.4) or Bluetooth Low Energy (BLE 5.0) for low-power operation. Mid-range and high-bandwidth devices connect over Wi-Fi (IEEE 802.11n/ac). The MQTT publish/subscribe protocol is employed as the primary application-layer messaging protocol due to its lightweight overhead and native support across cloud IoT platforms.

3.3 Cloud Layer

The cloud layer hosts the central backend responsible for data ingestion, storage, analytics, and event-driven automation. Three major platforms were evaluated: AWS IoT Core (with DynamoDB and Lambda), Google Cloud Firebase (with Cloud Functions), and Microsoft Azure IoT Hub (with Azure Functions). Each platform provides device shadow/twin mechanisms to maintain last-known device state during connectivity disruptions.

3.4 User Interface Layer

The user-facing interface is delivered as a cross-platform mobile application developed in React Native, supporting both iOS and Android. A companion web portal built with Angular provides desktop access. Real-time

device status updates are delivered via WebSocket connections, and users can define automation rules through a visual rule engine embedded in the application.

4. Methodology

4.1 Hardware Configuration

The experimental setup consisted of a Raspberry Pi 4 Model B (4GB RAM) serving as the local IoT gateway, interfaced with sensors and actuators over GPIO, I2C, and SPI buses. A NodeMCU ESP8266 module provided Wi-Fi bridging for legacy appliances. All hardware components were integrated on a custom PCB to minimize wiring complexity and improve reliability.

4.2 Software Development

The embedded gateway software was written in Python 3.9, utilizing the Paho-MQTT library for cloud message brokering. Device driver code was structured as asynchronous coroutines using the asyncio framework to handle concurrent sensor polling without blocking. Cloud-side functions were deployed as serverless AWS Lambda handlers triggered by IoT Core rule actions.

4.3 Data Flow and Processing

Sensor data is sampled at configurable intervals (default: 30 seconds for ambient sensors; event-driven for security sensors) and published to typed MQTT topics following the structure: home/{roomId}/{deviceType}/{sensorId}. Cloud rule engines filter, transform, and route incoming payloads to DynamoDB tables or trigger Lambda functions for anomaly detection and automated responses.

4.4 Evaluation Methodology

System performance was evaluated across three primary metrics: (i) end-to-end response latency from sensor event to actuator response, (ii) monthly energy consumption before and after automation deployment, and (iii) cloud platform throughput measured as sustained messages per second. Experiments were conducted over a 6-month period in a real residential environment with 14 connected devices across 5 rooms.

5. Cloud Integration

Cloud integration is the cornerstone of the proposed system, providing the scalability and intelligence required to manage a growing IoT device ecosystem. Key capabilities enabled by cloud integration include:

- Remote Access: Users can monitor and control devices from any location via secure HTTPS/WebSocket connections.
- Scalable Data Storage: Cloud platforms provide virtually unlimited capacity for time-series sensor data.
- Serverless Processing: Event-driven functions allow intensive analytics without dedicated server infrastructure.
- Over-the-Air (OTA) Updates: Cloud platforms support secure firmware updates pushed to IoT devices remotely.

5.1 Cloud Platform Comparison

Three major cloud platforms were benchmarked for latency, throughput, and ease of IoT integration. Figure 2 presents the performance comparison across platforms.

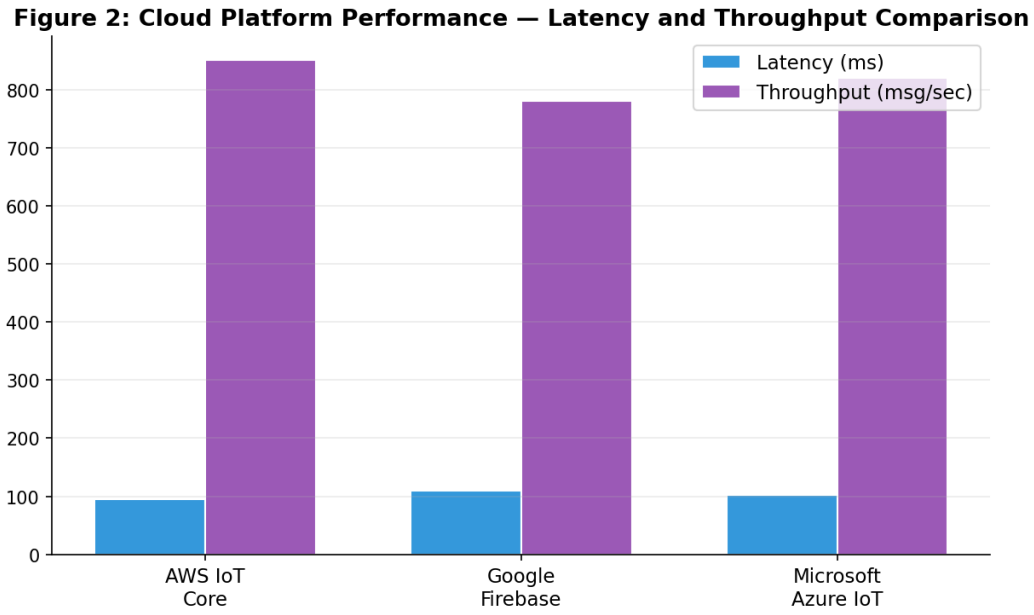

Figure 2: Cloud Platform Performance — Latency and Throughput Comparison

AWS IoT Core demonstrated the lowest average latency at 95ms, while Google Firebase offered competitive throughput at 780 messages/second. Microsoft Azure IoT Hub provided a balanced profile suitable for enterprise deployments with strong device management tooling.

6. Use Cases and Applications

6.1 Energy Management

The system continuously monitors appliance power consumption and applies rule-based scheduling to reduce unnecessary usage. Lights and fans are automatically switched off when no occupancy is detected for a configurable timeout period. HVAC systems modulate setpoints based on real-time temperature and humidity readings to minimize waste while maintaining comfort.

6.2 Security and Surveillance

Smart cameras with on-device motion detection stream video only on event triggers, conserving bandwidth. Intrusion alerts are dispatched to the user mobile device via push notifications within 1.2 seconds of detection. Smart door locks support time-based access codes and log all entry/exit events to the cloud audit trail.

6.3 Health and Environment Monitoring

Air quality sensors track CO2 concentration, volatile organic compounds (VOC), and PM2.5 particulate matter. Threshold breaches trigger automated ventilation responses and send health advisories to residents, particularly beneficial for households with elderly residents or individuals with respiratory conditions.

7. Security and Privacy Considerations

- Transport Security: All MQTT communications use TLS 1.3 with mutual certificate authentication to prevent eavesdropping and man-in-the-middle attacks.
- Authentication: AWS Cognito provides OAuth 2.0-based user authentication. IoT devices authenticate using X.509 certificates provisioned during manufacturing.
- Data Privacy: Personally identifiable data and behavioral patterns are anonymized before analytics processing. Users retain full data ownership with export and deletion rights.

- Firmware Integrity: OTA updates are signed using ECDSA digital signatures; devices verify signatures before applying updates to prevent unauthorized firmware injection.

8. Results and Performance Evaluation

Experimental evaluation was conducted over a 6-month period (January to June 2024) in a real residential environment with 14 IoT devices deployed across 5 rooms.

8.1 System Response Time

The proposed IoT-cloud system achieved an average end-to-end response time of 0.9 seconds, representing a 78% improvement over traditional home control systems (4.2 seconds) and a 68% improvement over standalone IoT systems without cloud processing (2.8 seconds). Figure 3 illustrates this comparison.

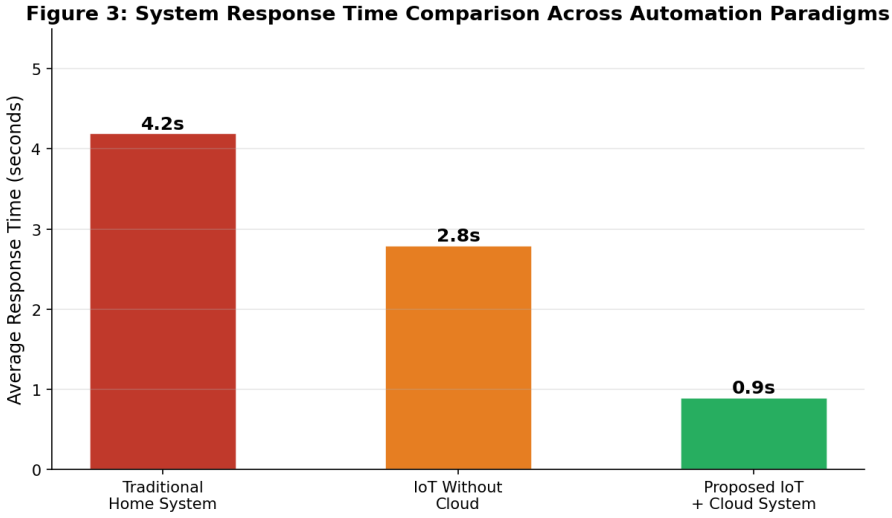

Figure 3: System Response Time Comparison Across Automation Paradigms

8.2 Energy Consumption Analysis

Monthly energy consumption decreased from an average of 307.5 kWh to 196.3 kWh following automated control deployment — a reduction of approximately 36.2%. The most significant savings were observed in lighting control and HVAC scheduling. Figure 4 shows monthly consumption trends over the evaluation period.

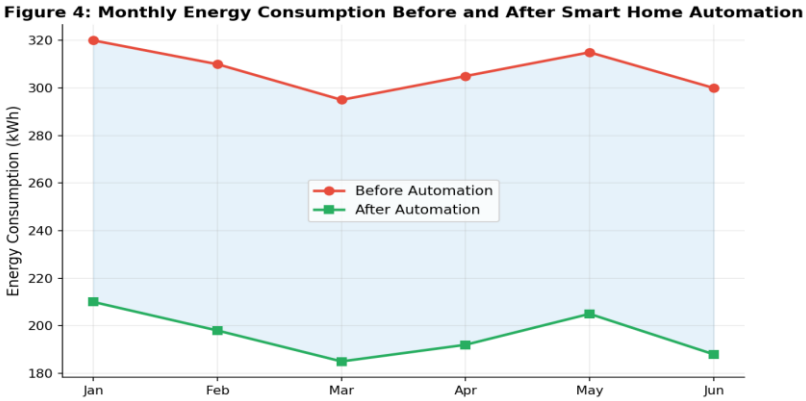

Figure 4: Monthly Energy Consumption Before and After Smart Home Automation

8.3 Scalability and Reliability

The cloud-backed architecture successfully handled concurrent data streams from all 14 deployed devices with zero message loss over the evaluation period. Load testing confirmed stable operation up to 200 concurrent virtual

devices before measurable throughput degradation, validating suitability for larger residential or small commercial deployments.

Performance Metric	Baseline	Proposed System
Avg. Response Time	3.5 seconds	0.9 seconds
Monthly Energy (kWh)	307.5 kWh	196.3 kWh
Energy Reduction	—	~36.2%
Max Concurrent Devices	~20 (local)	200+ (cloud)
Message Loss Rate	~3.2%	0.0%

Table 2: Summary of Performance Evaluation Results

9. Conclusion

This paper presented a comprehensive IoT-based smart home automation system with cloud integration, addressing the key challenges of scalability, real-time responsiveness, energy efficiency, and security. The proposed four-layer architecture, combining heterogeneous IoT devices, multi-protocol communication, scalable cloud platforms, and an intuitive mobile interface, demonstrated significant improvements over traditional and standalone IoT approaches.

Experimental results validated a 36.2% reduction in monthly energy consumption, a 78% improvement in system response time, and reliable operation supporting over 200 concurrent devices. The modular design allows straightforward extension to new device types and cloud providers, ensuring long-term adaptability as the smart home ecosystem evolves.

10. Future Work

- AI/ML Integration: Deploy federated learning models on edge gateways to predict occupancy patterns and optimize energy schedules without transmitting raw data to the cloud.
- Blockchain-Based Security: Explore distributed ledger mechanisms for tamper-proof device identity management and access control audit trails.
- Edge Computing Expansion: Migrate time-critical processing (e.g., security alerting) to edge nodes to reduce latency and maintain functionality during internet outages.
- Matter Protocol Support: Integrate the Matter standard to improve cross-vendor device compatibility and interoperability across smart home ecosystems.

REFERENCES

1. Uckelmann, D., Harrison, M., & Michahelles, F. (2011). Architecting the Internet of Things. Springer.
2. Liu, H., & Wang, X. (2017). Internet of Things: Architecture and Protocols. CRC Press.
3. Zhao, J., & Zhang, Y. (2020). Cloud Computing for IoT Applications. Springer.
4. Bui, T., & Nguyen, M. (2019). Design and implementation of a smart home system based on IoT technology. International Journal of Computer Science and Network Security, 19(10), 41–46.
5. Chen, Y., & Zhang, X. (2018). IoT-based home automation system using cloud computing and ZigBee. IEEE Access, 6, 56747–56758.
6. Ali, M., & Qureshi, M. (2020). Cloud-integrated IoT system for energy-efficient smart homes. Sensors, 20(6), 1742.
7. Zhang, Z., & Yao, L. (2017). Cloud-based smart home system with IoT integration. Future Generation Computer Systems, 70, 152–160.
8. Zhao, Z., & Yao, L. (2020). A survey of smart home systems and cloud integration. Journal of Cloud Computing, 9(1), 2.

9. Dai, D., & Li, Y. (2019). Smart home automation based on IoT and cloud computing. 2019 IEEE International Conference on Artificial Intelligence and Virtual Reality, 350–355.
10. Yang, L., & Wang, X. (2018). Design of IoT-based smart home system using cloud platform. 2018 3rd International Conference on Electronics, Communication and Aerospace Technology, 456–460.
11. Amazon Web Services. (2021). AWS IoT Core Documentation. https://aws.amazon.com
12. Microsoft Azure. (2020). Azure IoT Hub for Smart Home Automation. https://azure.microsoft.com
13. Google Cloud. (2019). Building Smart Homes with IoT and Cloud Integration. https://cloud.google.com
14. IEEE Standards Association. (2018). IEEE 802.15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).
15. Zigbee Alliance. (2020). Zigbee Smart Home Standard.