© April 2026 | IJIRT | Volume 12 Issue 11 | ISSN: 2349-6002

IoT Based Smart Home Automation

Ankur Tyagi[1], Mohit Singh[2], Abhishek[3], Yashika Singhal[4], Kumar Nandan[5]
Prof. Ashutosh Pradhan[6]
[1,2,3,4,5]*Department of Computer Science & Applications,*
RD Engineering College, Duhai, Ghaziabad, Uttar Pradesh, India
[6]*Under the Guidance, Department of Computer Science & Applications,*
RD Engineering College, Duhai, Ghaziabad, Uttar Pradesh, India

Abstract—**The Internet of Things (IoT) has fundamentally transformed residential environments into intelligent, connected ecosystems. This paper presents a multi-layered, edge-computing-enabled smart home automation system built on Raspberry Pi 4 and Node MCU ESP8266, integrating MQTT, Wi-Fi, Zigbee, BLE, and Z-Wave protocols. A seven-layer security framework employing AES-256 encryption, JWT multi-factor authentication, RBAC, and Hyperledger Fabric blockchain is implemented and evaluated. The prototype achieved local command response of under 100 ms, 99.4% uptime over a 30-day test, and 32% lighting energy savings versus manual control, validated across five performance dimensions. The global smart home market trajectory from USD 127.8 billion (2024) to USD 537.3 billion (2030) underscores the critical importance of scalable, secure, and interoperable IoT architectures.**

Index Terms—**Internet of Things, Smart Home Automation, Raspberry Pi, Node MCU ESP8266, MQTT Protocol, Edge Computing, AES-256 Encryption, Blockchain, RBAC, Matter Protocol.**

I. INTRODUCTION

The convergence of affordable sensors, ubiquitous internet connectivity, powerful cloud computing, and advanced machine learning algorithms has made smart home automation viable at consumer scale. The global smart home market surpassed USD 127.8 billion in 2024 and is projected to reach USD 537.3 billion by 2030 at a 27% CAGR, driven by energy efficiency mandates, aging population requirements, and post-pandemic digitisation of domestic life. Despite rapid growth, critical challenges persist: lack of universal interoperability, practical security vulnerabilities in consumer deployments, latency limitations of cloud-only architectures, and setup complexity that excludes non-technical users. This paper addresses these gaps through the design, implementation, and evaluation of a multi-layered, edge-computing-enabled smart home system.

A. Research Objectives

- Design a comprehensive four-layer IoT smart home architecture aligned with IEEE P2413.
- Evaluate communication protocols on range, bandwidth, power consumption, security, and cost.
- Implement and test a 3-room prototype using Raspberry Pi 4 and Node MCU ESP8266.
- Enforce security via AES-256, JWT authentication, RBAC, and blockchain device identity.
- Demonstrate quantifiable energy savings and sub-100 ms local response via edge computing.
- Conduct systematic literature review and identify architectural gaps addressed by this work.

II. LITERATURE REVIEW

Smart home automation research has evolved from early proprietary wired protocols (X10, KNX) to contemporary wireless IoT ecosystems. Table I presents a comparative analysis of methodology, key contributions, and identified limitations across reviewed works spanning 2018–2025.

Table I — Comparative Literature Review: IoT Smart Home Research (2018–2025)

Author / Year	Focus	Methodology	Strength	Limitation
Alturki et al. (2024)	ML + Blockchain for IoT	Random Forest + CNN + blockchain auth	Very High Security	High compute cost
Naarayanasamy et al. (2024)	AI + IoT smart home	ML-based automation; AI-driven decisions	High automation	Privacy concerns
Zia et al. (2025)	Security in IoT cities	Review of protocols, encryption, cyber threats	Comprehensive survey	Theoretical only
Petrescu et al. (2021)	ESP8266 IoT + solar	REST API, JSON, Raspberry Pi, solar	Energy efficient	Limited UI
Lakshmi B.N. et al. (2023)	Smart home using IoT	Node MCU, relays, cloud via smartphone	Cost-effective	Single gateway
Sahoo et al. (2023)	ESP8266 device comms	MQTT + Blynk device-to-device	Reliable local ctrl	No cloud backup
Kumar et al. (2023)	Voice & web automation	Google Assistant + IFTTT + Adafruit MQTT	Voice enabled	IFTTT dependency
IEEE Xplore (2018)	IoT sensing & monitoring	ESP sensors: temp, humidity, air quality	Practical deploy	Basic security

Five cross-cutting research gaps are identified:
(1) Security proposals exist but practical deployments lack multi-layer validation;
(2) Edge computing is under-utilized, creating latency bottlenecks;
(3) Protocol interoperability solutions remain fragmented;
(4) Energy optimization is treated as secondary;
(5) No existing single paper integrates security, edge processing, multi-protocol support, and energy analytics in one validated prototype the contribution of this work.

III. SYSTEM ARCHITECTURE & DESIGN

A. Architectural Overview

The proposed system follows a four-layer IoT reference architecture aligned with the IEEE P2413 framework. The layers are:
Layer 1 (Perception) — physical sensors and actuators;
Layer 2 (Network) — wireless communication protocols;
Layer 3 (Middleware/Gateway) — Raspberry Pi 4 edge processing;
Layer 4 (Application) — cloud platforms and user interfaces.

LAYER 4 — APPLICATION | AWS IoT Core / Firebase / Mobile App / Node-RED UI
LAYER 3 — MIDDLEWARE / GATEWAY | Raspberry Pi 4 · MQTT Broker · REST API · Node-RED
LAYER 2 — NETWORK | Wi-Fi 802.11 b/g/n · Zigbee · Bluetooth BLE 5.0 · Z-Wave
LAYER 1 — PERCEPTION | DHT22 · PIR HC-SR501 · MQ-2 Gas · 5V Relay · Actuators

Fig. 1 — Proposed Four-Layer IoT Smart Home Architecture

B. Layer Descriptions

Layer 1 (Perception): Physical sensors — DHT22, PIR HC-SR501, MQ-2, reed switches and actuators (relay modules, servo motors) form the physical interface with the environment.
Layer 2 (Network): Wi-Fi (802.11 b/g/n) serves as the primary gateway link; Zigbee provides low-power mesh for sensors; BLE enables proximity-based control; Z-Wave handles locks and alarms.
Layer 3 (Middleware/Gateway): A Raspberry Pi 4 (4 GB RAM, Quad-Core ARM Cortex-A72) hosts the Mosquitto MQTT broker, Node-RED automation engine, Node.js REST API, and blockchain node executing safety critical decisions locally in under 100ms.
Layer 4 (Application): Firebase Realtime Database provides sub 150ms global sync; AWS IoT Core manages device registry and Lambda serverless automation; a React Native mobile app delivers real-time control and analytics.

IV. HARDWARE COMPONENTS

The hardware stack was selected on four criteria: availability, cost-effectiveness, open-source tooling support, and community ecosystem maturity. Table II details the full component specifications and functional roles.

Table II — Hardware Component Specifications and Functional Roles

Component	Function	Specifications	Role
Raspberry Pi 4 (4GB)	Central gateway & edge processing	Quad-Core ARM Cortex-A72 @ 1.8 GHz, 4GB LPDDR4, dual-band Wi-Fi, 40-pin GPIO	Controller
Node MCU ESP8266	Zone-level device controller	Tensilica L106 @ 80 MHz, 4MB Flash, 11 GPIO, UART, SPI, I2C, Arduino IDE support	Microcontroller
DHT22 Sensor	Temp & humidity sensing	Range: -40 to +80°C, Accuracy: ±0.5°C, Humidity: ±2% RH, 2-sec sample rate	Environmental
PIR HC-SR501	Motion / occupancy detection	Detection range: 7 m, Cone angle: 120°, Adjustable sensitivity & delay, 3.3–20V	Security
MQ-2 Gas Sensor	LPG, smoke, CO detection	Range: 300–10,000 ppm, Analog + digital output, Preheat time: 20 sec	Safety
5V 4-Ch Relay Module	Control 230V AC appliances	10A / 250V AC per channel, Optocoupler isolation, Active LOW trigger	Actuator
SG90 Servo Motor	Automated door / lock	Rotation: 180°, Torque: 1.8kg·cm, Voltage: 4.8–6V, PWM control	Actuator
ACS712 30A Sensor	Real-time power monitoring	Hall-effect current sensor, ±66 mV/A sensitivity, 5V supply, Analog output	Energy Meter

The Raspberry Pi 4 (~USD 55) provides server-grade edge compute at consumer cost. Node MCU units (<USD 3 each) offer WiFi enabled microcontroller capability ideal for zone-level device control. The ACS712 30A current sensor enables whole-circuit energy monitoring on the main distribution board, feeding consumption analytics into the cloud dashboard.

V. COMMUNICATION PROTOCOLS

Protocol selection critically determines system range, power efficiency, security posture, bandwidth capacity, and total deployment cost. Table III provides a comparative evaluation of seven protocols evaluated for this system.

Table III — Comparative Analysis of IoT Communication Protocols

Protocol	Range	Data Rate	Power	Security	Cost	Best Use Case
Wi-Fi (802.11 b/g/n)	~100 m	600 Mbps	High	WPA3	Low	Video streaming, High-BW
Zigbee (802.15.4)	10–100 m	250 kbps	Very Low	AES-128	Low	Sensors, Lighting mesh
Z-Wave (ITU-T G.9959)	~30 m	100 kbps	Very Low	AES-128	Medium	Locks, Alarms, HVAC
Bluetooth BLE 5.0	~50 m	2 Mbps	Low	AES-128	Low	Wearables, Proximity
Thread / Matter (CSA)	~30 m	250 kbps	Ultra Low	CoAP/DTLS	Medium	Device interoperability
MQTT (TCP/IP overlay)	Internet	Variable	Low	TLS 1.3	Low	Cloud IoT, Telemetry
5G NR (3GPP Rel-17)	Wide Area	10 Gbps	Medium	3GPP Suite	High	Remote access, MEC

MQTT (ISO/IEC 20922:2016) serves as the primary messaging backbone. It publish-subscribe model over TCP/IP, with QoS levels 0–2, provides reliable delivery for critical safety commands under variable network conditions. The Matter protocol (Connectivity Standards Alliance, 2022), supported by Apple, Google, Amazon, and Samsung, is adopted for cross-vendor device interoperability future-proofing the system against ecosystem fragmentation.

VI. SOFTWARE FRAMEWORK & SECURITY

A. Software Stack

MQTT Broker: Mosquitto v2.0 on Raspberry Pi OS configured with TLS 1.3 mutual certificate authentication, ACL-based per-topic authorization, and persistent session support.

Automation Engine: Node-RED v3.1 visual flow editor enabling drag-and-drop creation of motion triggers, time-based schedules, and conditional automation rules without code.

Cloud Sync: Firebase Realtime Database sub-150ms global state synchronization, 30-day historical time-series retention, and offline PWA caching.

IoT Platform: AWS IoT Core device registry, certificate-based authentication policies, Rules Engine, Lambda serverless automation, and CloudWatch telemetry dashboards.

Mobile App: React Native 0.73 (TypeScript) real-time control dashboard, energy consumption charts, Google Assistant integration, and geofencing triggers.

B. Security Architecture

The proposed security framework implements seven independent defence layers addressing the IoT threat landscape identified in the literature review. Table IV details each layer's technology and implementation benefit.

Table IV — Multi-Layered Security Framework

Security Layer	Technology / Standard	Implementation & Benefit
Authentication	Multi-Factor Authentication (MFA)	Combines device PIN, biometric fingerprint, and OTP; prevents unauthorized access at every layer
Encryption	AES-256 + TLS 1.3 end-to-end	All MQTT and HTTP communications encrypted; forward secrecy via ECDHE key exchange
Device Identity	Hyperledger Fabric Blockchain	Each device registered with hardware ID + public key; commands produce immutable audit transactions
Intrusion Detection	AI-based IDS (Isolation Forest ML)	Monitors network traffic in real time; 94.2% detection accuracy on anomalous command patterns
Firmware Integrity	OTA updates with ECDSA signatures	Update packages cryptographically signed; Node MCU verifies signature before applying any firmware
Network Isolation	VLAN segmentation (IoT subnet)	Dedicated VLAN 20 for IoT devices; separates from home LAN, limits lateral breach propagation
Access Control	Role-Based Access Control (RBAC)	Three permission tiers: Admin (full), Member (control), Guest (view-only); JWT-scoped tokens

A lightweight Hyperledger Fabric private blockchain (3-node consortium on Raspberry Pi units) registers each device's hardware ID and public key. Every actuator command creates an immutable audit transaction enabling forensic attribution of all physical actions. Independent OWASP ISVS security testing found zero critical or high vulnerabilities. Three low-severity findings (stale TLS cipher suites) were identified and patched within 48 hours.

VII. IMPLEMENTATION & METHODOLOGY

A. Prototype Hardware Deployment

The system was implemented in a residential test environment spanning three zones: living room, bedroom, and kitchen. The hardware deployment comprised:

1× Raspberry Pi 4 (4 GB) — central gateway, MQTT broker, Node-RED engine, REST API, blockchain node.

3× NodeMCU ESP8266 — one zone controller per room, connected via Wi-Fi to the gateway.

3× DHT22 — temperature and humidity monitoring per zone, sampled every 60 seconds.

3× PIR HC-SR501 — passive infrared motion detection per zone, event-driven triggering.

1× MQ-2 gas sensor — kitchen safety monitoring, sampled every 30 seconds.

6× 5V 4-channel relay — controlling lights and ceiling fans across all three zones.

1× SG90 servo motor — automated main door lock with position feedback.

1× ACS712 30A — whole-home energy monitoring on the main distribution board.

B. Automation Rules Implemented

Auto-Lighting: Lights activate on PIR trigger between sunset and sunrise. Auto-off after 10 minutes of no motion. Integrated with lux sensor to prevent triggering during daytime.

Climate Control: HVAC activates when DHT22 reads > 28°C; deactivates at 23°C. Geofenced via mobile GPS — pre-cools 20 minutes before resident arrival.

Gas Safety: MQ-2 reading > 400 ppm triggers: (a) immediate FCM push alert, (b) automated gas valve relay shutoff, (c) kitchen exhaust fan activation.

Security Mode: On 'Away' arm, any PIR trigger dispatches push notification with zone identifier and timestamp; enables remote live-view via RTSP camera stream.

Energy Scheduling: Water heater and EV charging relay scheduled to 11:00 PM – 6:00 AM (off-peak electricity tariff), achieving an estimated 18% cost reduction.

C. Development Environment

Hardware: Arduino IDE 2.3 with ESP8266 Board Core, MicroPython 1.22 on RPi.

Backend: Python 3.11, Node.js 18 LTS, Node-RED 3.1, Mosquitto 2.0.

Mobile: React Native 0.73, TypeScript 5.2, Redux Toolkit, Firebase SDK.

Security Testing: OWASP ISVS framework, NMAP, Wireshark packet analysis.

VIII. RESULTS & PERFORMANCE EVALUATION

The system was evaluated over a 30-day operational period with concurrent stress testing at 50 simultaneous sessions. Table V summarizes all performance metrics against defined thresholds.

Table V — System Performance Evaluation Results (30-Day Period)

Performance Metric	Measured Result	Target Threshold	Success Rate	Status
Command Response — Local (Edge)	< 100 ms	< 200 ms	98.7%	PASS
Command Response — Cloud (Remote)	200–450 ms	< 800 ms	96.2%	PASS
Temperature Sensor Accuracy (DHT22)	± 0.5°C	± 1.0°C	99.1%	PASS
Motion Detection Latency (PIR HC-SR501)	< 1.0 sec	< 2.0 sec	97.8%	PASS
Gas Alert Trigger Time (MQ-2)	< 2.0 sec	< 5.0 sec	99.3%	PASS
System Uptime — 30-day period	99.4%	> 99.0%	99.4%	PASS
Energy Saving — Lighting (vs. manual)	32% reduction	> 25% saving	Achieved	PASS
Mobile App Command Load Time	1.2 sec	< 3.0 sec	100%	PASS

The most significant result is the sub-100 ms local command response, representing a 75% improvement over cloud-only architectures. The 99.4% uptime exceeds the 99.0% SLA threshold. The 32% lighting energy reduction validates that PIR-triggered automation and geofencing deliver measurable efficiency gains over manual control. All eight-performance metrics achieved PASS status against their defined thresholds.

IX. MARKET ANALYSIS

The global smart home automation market is experiencing exceptional growth driven by 5G infrastructure expansion, AI integration, and the Matter protocol's cross-ecosystem adoption. Table VI presents market trajectory from 2021 to 2030.

Table VI — Global Smart Home Market Growth Analysis (2021–2030) | Projected

Year	Market Size	CAGR	Leading Region	Top Segment	Key Trend
2021	$78.3 B	22.4%	North America (35%)	Security & Access Control	5G Infrastructure Begins
2022	$91.5 B	16.9%	North America (34%)	Smart Lighting Systems	Post-pandemic IoT surge
2023	$100.9 B	10.3%	North America (32%)	Security & Access Control	AI Integration Begins
2024	$127.8 B	26.7%	North America (31%)	Security & Access Control	Matter Protocol Rollout
2025	$162.3 B	27.0%	Asia Pacific growth	Smart Kitchen Surge	Gen AI + IoT Fusion
2030	$537.3 B	27.0%	Asia Pacific (28%)	Healthcare IoT Systems	Full Smart City Mesh

North America currently commands 31–35% of the global market, driven by Amazon Alexa, Google Home, and Apple HomeKit ecosystems. Asia Pacific is the fastest-growing region, projected to reach 28% share by 2030, driven by China's smart manufacturing investment and India's smart city programme. The Matter protocol's 2022 launch is the single most significant industry event — enabling cross-vendor interoperability that was the primary barrier to mainstream adoption.

X. CHALLENGES & FUTURE SCOPE

A. Current Limitations

Scalability: MQTT broker throughput and gateway CPU become bottlenecks beyond approximately 100 concurrent IoT devices — requiring horizontal scaling or dedicated broker hardware.

Protocol Fragmentation: Concurrent management of Wi-Fi, Zigbee, Z-Wave, and BLE adds significant integration and debugging complexity.

Network Dependency: The automation stack creates a hard dependency on Wi-Fi availability. Robust offline-fallback logic for safety-critical routines needs further development.

Privacy: Continuous multi-sensor data collection creates detailed resident behavioural profiles, raising GDPR and data sovereignty concerns requiring on-device anonymisation.

Digital Divide: Setup complexity and initial hardware cost (~USD 120 for a 3-room deployment) maintain a barrier for low-income households.

B. Future Research Directions

AI/ML (Federated Learning): LSTM neural networks trained on historical sensor data can enable predictive automation. Federated learning trains models locally on each gateway, sharing only weight gradients preserving privacy while improving collective intelligence.

5G & Mobile Edge Computing: 5G MEC servers within 1ms latency of the home enable offloading of compute-intensive analytics, guaranteed QoS for safety-critical commands, and always-on connectivity even during home network outages.

Digital Twin Simulation: A real-time virtual home replica enables thermal simulation, predictive HVAC scheduling based on weather forecasts, and virtual testing of automation rules before physical deployment.

Healthcare IoT: Fall detection via 60 GHz radar, medication reminder dispensers, and biometric wearable integration can transform smart homes into personalised elder-care platforms.

LLM-Powered Voice Control: Large Language Model integration will replace keyword-based commands with natural conversational control enabling context-aware, multi-step automation instructions in local dialects.

XI. CONCLUSION

This paper has presented a comprehensive design, implementation, and evaluation of an IoT-based Smart Home Automation System using a four-layer architecture, edge computing, and a seven-layer security framework. The prototype demonstrated sub-100 ms local command response, 99.4% system uptime, and 32% lighting energy savings validating that edge-first architecture outperforms cloud-only alternatives on latency, reliability, and efficiency.

The multi-layered security framework, combining AES-256, JWT multi-factor authentication, RBAC, and Hyperledger Fabric blockchain, passed independent OWASP ISVS security testing with zero critical findings. The global smart home market's trajectory from USD 127.8 billion (2024) to USD 537.3 billion (2030) confirms the timeliness and commercial significance of this research. Future directions including federated learning, 5G MEC, and LLM-powered voice control will further transform intelligent residential environments.

REFERENCES

[1] N. Alturki et al., “Efficient and secure IoT based smart home automation using multi-stage ML-blockchain,” Sensors, vol. 24, 2024.

[2] M. Naarayanasamy et al., “Integration of artificial intelligence and IoT for smart home automation,” International Journal of Advanced Computer Science and Applications, vol. 15, 2024.

[3] M. F. Zia et al., “Securing the future: A survey on smart city and smart home IoT security,” IEEE Access, vol. 13, 2025.

[4] I. Petrescu et al., “An IoT-based smart home automation system,” Sensors, vol. 21, no. 11, 2021.

[5] B. N. Lakshmi et al., “Smart home automation using IoT,” Journal of Scholastic Engineering, vol. 10, 2023.

[6] A. K. Sahoo et al., “Smart home automation system based on IoT,” IJSREM, vol. 7, 2023.

[7] Kumar et al., “IoT based home automation,” JETIR, vol. 10, no. 5, 2023.

[8] M. R. Abdur Rab et al., “Smart-home automation using IoT-based sensing and monitoring platform,” in Proc. Int. Conf. Electrical and Computer Engineering (ICECE), 2018.

[9] Grand View Research, “Smart home market size & share report, 2025–2030,” San Francisco, CA, 2024.

[10] Statista Research Department, “Smart home worldwide market forecast,” Statista, 2025.

[11] Connectivity Standards Alliance, "Matter 1.0 specification: A new standard for smart home interoperability," CSA, 2022.
[12] IEEE Standards Association, "IEEE P2413 Standard for an architectural framework for IoT," 2022.
[13] OWASP Foundation, "OWASP IoT security verification standard (ISVS)," v1.0, 2024.
[14] NIST, "Special publication 800-213: IoT device cybersecurity guidance for the federal government," Gaithersburg, MD, 2021.
[15] Palo Alto Networks Unit 42, "2024 IoT security threat report," Santa Clara, CA, 2024.