Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

A Review on IoT-Based Smart Home Automation Systems: Technologies, Architectures, and Challenges

Swarit Kori
Dept. of Electronics & Telecommunication Engineering
Jabalpur Engineering College (JEC), Jabalpur, India

Rounak Manglani
Dept. of Electronics & Telecommunication Engineering
Jabalpur Engineering College (JEC), Jabalpur, India

Abstract - The Internet of Things (IoT) has emerged as a transformative force in residential automation, enabling unprecedented levels of energy efficiency, safety monitoring, and remote device control. This paper presents a systematic review of eight recent peer-reviewed studies on IoT-based smart home automation systems, examining architectures ranging from cloud-dependent microcontroller platforms to localized edge computing frameworks. Each system is analyzed across key dimensions: hardware architecture, communication protocols, artificial intelligence integration, security frameworks, deployment model, and cost-effectiveness. A structured comparative analysis reveals three critical and recurring gaps in the literature — the near-absence of genuine AI-driven automation (only one of eight systems employs a deep learning model), pervasive reliance on basic cloud security that leaves the majority of systems vulnerable to cyberattacks, and persistent protocol fragmentation that prevents seamless cross-device interoperability. Based on these findings, a unified future research direction is proposed that integrates edge computing, predictive deep learning, universal communication standards, and blockchain-based decentralized security, collectively enabling the transition from remotely controlled devices to truly autonomous and secure intelligent living environments.

Keywords — Internet of Things (IoT); Smart Home Automation; Edge Computing; Machine Learning; Blockchain Security; Communication Protocols; NodeMCU; Raspberry Pi; ESP32; Energy Management

I. INTRODUCTION

The Internet of Things (IoT) represents one of the most consequential technological developments in modern electronics and telecommunications engineering. By embedding physical objects with sensors, actuators, and wireless connectivity, IoT enables autonomous data collection, machine-to-machine communication, and real-time actuation without direct human intervention [1]. As of 2023, the global count of connected IoT devices has surpassed the world's human population, indicating a fundamental shift in the relationship between the physical environment and digital infrastructure. Practical applications now span five broad domains: healthcare, precision agriculture, smart homes, smart cities, and industrial automation.

Within these domains, smart home automation has emerged as one of the most immediately impactful application areas. Low-cost microcontroller platforms and edge computing architectures have demonstrated substantial improvements across multiple residential dimensions, including energy conservation, real-time emergency detection, indoor environmental comfort, and secure remote control from anywhere in the world [2][5][8]. Contemporary systems now enable a single smartphone to manage thermal regulation, gas leak detection, occupant health monitoring, electricity billing oversight, and voice-commanded appliance management — all simultaneously.

Despite this progress, three fundamental challenges remain largely unresolved in the smart home domain: security vulnerabilities, communication protocol fragmentation, and the near-complete absence of genuine AI-driven autonomy. With only one of the eight systems reviewed in this study incorporating machine learning-based decision-making and blockchain security [1][4], the majority of so-called ‘smart’ homes continue to function primarily as remote-controlled switching networks rather than truly autonomous environments.

The principal contributions of this paper are: (i) a systematic, multi-dimensional comparative analysis of eight recent peer-reviewed IoT smart home implementations spanning 2018–2023; (ii) structured identification of three recurring research gaps — limited AI integration, inadequate security, and protocol fragmentation; and (iii) a synthesized future architecture roadmap combining edge computing, deep learning, universal protocols, and blockchain security into a cohesive next-generation smart home design.

II. METHODOLOGY

Papers reviewed in this study were sourced from high-authority academic databases and open-access journals, including IEEE Xplore, PubMed Central (PMC), MDPI, and IJRASET, covering the publication period from 2018 to 2023. This range was selected to capture both foundational benchmark studies and the most recent implementation advances. The combination of sources ensures balanced representation of both rigorously peer-reviewed high-impact research and practical engineering implementations that reflect real-world deployment constraints.

A paper was included if it satisfied at least two of the following criteria. First, technical diversity: studies were selected to represent a range of hardware architectures, from high-power edge computing platforms such as Raspberry Pi to ultra-low-cost microcontrollers such as ESP32 and NodeMCU, deliberately avoiding redundant coverage of identical hardware configurations. Second, problem-solving distinctness: priority was given to studies addressing unique real-world challenges — energy metering, emergency gas

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

leak detection, health vital monitoring, communication protocol evaluation, and cybersecurity — rather than studies solving the same problem with minor variations.

Each selected paper was then systematically analyzed across seven evaluation dimensions: (1) hardware framework, (2) communication protocol(s) employed, (3) degree of artificial intelligence integration, (4) security mechanism, (5) deployment model (cloud vs. edge), (6) cost-effectiveness, and (7) primary unique contribution. This structured approach enabled consistent cross-paper comparison and facilitated the identification of recurring capability gaps and emerging trends across the reviewed literature.

III. LITERATURE REVIEW

Chataut et al. [1] provided one of the most comprehensive contemporary surveys of IoT applications, systematically covering five major sectors: healthcare, agriculture, smart homes, smart cities, and industrial IoT. Rather than proposing a new system, the authors synthesized the state of the field to identify the three most critical barriers to widespread IoT deployment: security and privacy vulnerabilities, cross-platform interoperability deficits, and the growing challenge of managing data volumes at scale. Their central conclusion was that universal communication standards and mature edge computing infrastructures are prerequisites for safely expanding the global network of connected devices.

Yar et al. [2] proposed a tightly integrated smart home solution built around the Raspberry Pi 3B, organized into a five-layer edge computing hierarchy that handles perception, communication, processing, storage, and application functions locally. This localized architecture eliminated dependence on cloud round-trips and delivered measurable performance improvements: end-to-end system response time was recorded at 15 milliseconds, and daily household energy consumption was reduced by 38% relative to manually operated homes. The authors acknowledged that reliance on dedicated local hardware introduces maintenance burdens and upfront costs, but maintained that edge-first design is the only path to achieving both responsiveness and data privacy simultaneously.

The study documented in [3] took a purely evaluative approach, conducting a rigorous comparative analysis of the five dominant smart home wireless protocols: Wi-Fi, Zigbee, LoRa, Z-Wave, and EnOcean. Each protocol was assessed across four dimensions — operating range, power consumption, data throughput, and inherent security. The analysis conclusively demonstrated that no single protocol satisfies all smart home use cases; Wi-Fi excels in throughput but is power-hungry, while Zigbee and Z-Wave offer better energy efficiency but limited range. The authors advocated for energy-harvesting technologies such as EnOcean and called for the establishment of an overarching universal communication standard as the IoT ecosystem matures.

Umer et al. [4] presented the most technically advanced system in this review, combining Arduino and Raspberry Pi hardware with two distinct intelligence layers: a Convolutional Neural Network (CNN) for automated classification of appliance operational states, and a blockchain-based decentralized authentication mechanism for securing device access. The CNN component eliminated the need for manual appliance management, while blockchain processing removed the single-point-of-failure vulnerability inherent in centralized cloud authentication. Testing in a controlled laboratory environment confirmed robust performance, although the authors noted that the computational overhead of blockchain consensus protocols remains a significant constraint on low-power IoT hardware.

Suryadevara et al. [5] addressed indoor environmental quality monitoring using the NodeMCU ESP8266, a low-cost Wi-Fi-enabled microcontroller paired with the open-source EmonCMS cloud dashboard. Their system tracked three comfort dimensions simultaneously: thermal conditions (temperature and humidity), visual comfort (ambient light levels), and hygienic conditions (air quality index). Real-time sensor data was accessible globally through a mobile interface, enabling remote monitoring and control. While the platform demonstrated that professional-grade environmental monitoring is achievable in developing-country households at minimal cost, the authors acknowledged the absence of predictive automation and the use of only basic transport-layer security.

The system described in [6] pursued a multifunctional integration strategy using the ESP32 microcontroller as a central hub. Beyond appliance control, the system incorporated a custom energy metering module with emergency gas and seismic shutoff capability, and a health monitoring module capable of measuring heart rate, blood oxygen saturation (SpO2), and core body temperature. Natural language voice control was achieved through an Amazon Alexa integration built on Voiceflow's NLP platform, with all operational data visualised on a Blynk cloud dashboard. The authors demonstrated that thoughtful integration of commodity open-source hardware with commercial voice AI services can deliver personalized, feature-rich smart home experiences at comparatively low total cost.

Ramya and Palaniappan [7] developed an IoT-based smart energy metering system targeting the specific problem of electricity billing transparency, employing an Arduino board instrumented with calibrated voltage and current sensors directly interfaced to a residential power line. The system generated real-time per-appliance billing data visible simultaneously to the homeowner and to the utility provider, enabling remote anomaly detection and potential power theft identification. The authors acknowledged a significant security limitation: the absence of data encryption over the transmission channel leaves billing data and device commands susceptible to interception or tampering, a vulnerability that must be addressed before real-world deployment.

Kumar et al. [8] designed a cost-effective, safety-oriented automation system based on the ESP32 microcontroller and L298N motor driver module for relay-based appliance switching, integrated with the Blynk IoT platform for mobile monitoring and control. The system's distinguishing characteristic was its dual-mode operation: normal remote appliance control could be instantly overridden by real-time fire and gas leakage alerts, which triggered both notifications and automatic shutoffs. Despite this practical safety-first design, the authors recognized that the system's automation logic remained fundamentally reactive — responding to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

detected events rather than predicting and preventing them — which limits its potential for true autonomous operation.

IV. COMPARATIVE ANALYSIS

Table I presents a structured cross-dimensional comparison of all eight reviewed systems, enabling direct identification of technological trends, recurring capability gaps, and design trade-offs across the current smart home automation landscape.

TABLE I. Comparative Analysis of Reviewed IoT-Based Smart Home Automation Systems

Ref.	Authors	Hardware	Protocol(s)	AI Used	Security	Deployment	Key Contribution / Unique Feature
[1]	Chataut et al.	General IoT Survey	Various	No	Basic	Cloud/Edge	Comprehensive five-domain IoT survey; identified three universal adoption barriers
[2]	Yar et al.	Raspberry Pi 3B	MQTT	No	Medium	Edge	Five-layer edge architecture; 15 ms latency; 38% daily energy reduction
[3]	Chataut, Sharma&Mukhopadhyay	Survey(Protocol)	Wi-Fi, Zigbee, LoRa, Z-Wave, EnOcean	No	N/A	N/A	Protocol comparison across range, power, data rate, and security; EnOcean energy harvesting
[4]	Umer et al.	RPi + Arduino	HTTP/Web	Yes (CNN)	High (Blockchain)	Edge	CNN appliance classification; blockchain decentralised authentication
[5]	Suryadevara et al.	NodeMCU ESP8266	Wi-Fi	No	Basic	Cloud	Thermal, visual, and hygienic comfort monitoring via EmonCMS dashboard
[6]	Sanjay et al.	ESP32	Wi-Fi	Partial (NLP)	Basic	Cloud	Health vitals tracking; Alexa voice control; gas/earthquake shutoff
[7]	Ramya & Palaniappan	Arduino	Wi-Fi/Web	No	Basic	Cloud	Real-time electricity billing; power theft detection for utility providers
[8]	Kumar et al.	ESP32 + L298N	Wi-Fi	No	Basic	Cloud	Dual-mode fire/gas safety alerts with automatic appliance shutoff

Several significant patterns emerge from the comparative data. Wi-Fi dominates as the communication protocol across six of the eight systems, reflecting its ubiquity and ease of integration, but at the cost of higher idle power consumption relative to alternatives such as Zigbee or LoRa identified in [3]. Edge computing deployment is adopted by only two systems [2][4], while the remaining six depend on cloud platforms, introducing latency penalties and data privacy concerns. Most critically, genuine machine learning integration appears in only one system [4] — despite 'smart' being applied uniformly to all eight — exposing the substantial gap that persists between marketing language and the technical reality of autonomous, learned automation.

V. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

A. Security Vulnerabilities in Smart Home Systems

A critical finding of this review is that six of the eight analyzed systems rely exclusively on basic cloud security frameworks — typically transport-layer SSL/TLS without additional authentication or encryption at the application layer — a configuration that represents a significantly underappreciated risk in the residential context. Unlike conventional enterprise cybersecurity breaches that compromise stored data, smart home security failures have direct physical consequences. A successful intrusion into a compromised system could enable remote unlocking of entry points, covert surveillance through embedded indoor cameras, deliberate disabling of fire and gas detection subsystems, and long-term behavioral profiling of occupants from energy usage patterns [1][4]. Only one reviewed system [4] addressed this threat surface through blockchain-based decentralized authentication, which eliminates the central identity server as a single point of compromise. This finding underscores the urgent need for standardized, multi-layer security frameworks as baseline requirements rather than optional enhancements in smart home implementations.

B. Limited AI Integration

Despite the pervasive application of the term 'smart home' across the literature, this review reveals that genuine artificial intelligence remains largely absent from current implementations. Only one of the eight systems employed a real machine learning model — specifically, a Convolutional Neural Network for automated classification of appliance operational states [4]. The remaining seven systems function as remotely operated switching networks, requiring continuous manual input from users for every state change. A genuinely intelligent home automation system should instead autonomously learn the occupant's behavioral patterns over time and proactively optimize indoor conditions — adjusting temperature, lighting, and appliance states — without requiring active user intervention. The absence of predictive AI represents the single largest gap between the current state of smart home technology and its transformative potential.

C. Protocol Fragmentation and Interoperability

The heterogeneous landscape of communication protocols across this review — Wi-Fi, Zigbee, Z-Wave, LoRa, MQTT, and HTTP — constitutes a fundamental structural barrier to seamless smart home deployment at scale. As demonstrated in [3], no single protocol simultaneously satisfies the full spectrum of smart home requirements across range, power consumption, data rate, and security. The practical consequence of this fragmentation is that consumers must maintain multiple parallel and mutually incompatible ecosystems within a single home, each demanding dedicated protocol gateways and separate mobile applications. This fragmentation raises total system cost, increases the likelihood of integration failures, and forms one

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

of the most significant deterrents to mainstream smart home adoption globally.

D. Future Research Directions

Based on the synthesis of all eight reviewed systems, the next generation of smart home automation must integrate the strongest elements identified in the literature into a single unified architecture. Specifically, future systems should incorporate: (1) a localized edge computing platform to eliminate cloud round-trip latency and preserve occupant data privacy [2]; (2) deep learning models for predictive behavioral modeling and proactive energy optimization, enabling the home to anticipate and respond to occupant needs without prompting [4]; (3) natively integrated life-safety subsystems for fire, gas, and health emergency detection and response [6][8]; (4) a universal communication protocol abstraction layer ensuring cross-manufacturer and cross-generation device interoperability [3]; and (5) a blockchain-based decentralized security framework providing cryptographically verifiable authentication and tamper-proof access logs [4]. The realization of such a unified architecture would represent a genuine transition from remotely controlled residences to truly autonomous, privacy-preserving, and secure intelligent living environments.

VI. CONCLUSION

This systematic review demonstrates that IoT-based smart home automation has progressed well beyond basic appliance convenience, with documented contributions in edge computing efficiency, real-time life safety monitoring, and energy consumption transparency. However, a fundamental ceiling on real-world impact remains: the majority of current implementations continue to rely on fragmented communication protocols and minimal cloud security frameworks, while genuine AI-driven predictive automation is demonstrably present in only one of the eight systems reviewed.

The trajectory of the field must shift decisively from building more sophisticated remote-control switching systems toward holistic architectures that integrate predictive deep learning for behavioral automation, universal communication standards for seamless cross-device interoperability, and decentralized security frameworks — such as blockchain — that protect both the data and the physical integrity of the home environment. Only through this convergence can the smart home evolve from a consumer convenience product into a truly autonomous, resilient, and intelligent living system.

Declaration of AI Assistance

In accordance with the IJERT AI Usage Policy, the authors declare that Claude AI (Anthropic) was employed as a writing assistance tool during the preparation of this manuscript. AI assistance was used specifically for: (1) language refinement, grammar correction, and academic register improvement of author-drafted content; (2) formatting and structural organization of sections in accordance with IJERT template requirements; and (3) polishing of author-written paragraph drafts into formal academic prose.

All eight source papers were independently identified, accessed, and read by the authors of this study. All paper summaries, comparative findings, research gap identification, and conclusions represent the authors' original intellectual contributions. The comparative analysis table was constructed by the authors based on their independent reading of all reviewed studies. All references have been verified by the authors and correspond to genuine published works.

AI tools were not used to generate scientific analyses, fabricate data or citations, conduct literature searches, or make intellectual judgments regarding research gaps or conclusions. The authors assume full responsibility for the accuracy, originality, and integrity of this manuscript.

REFERENCES

[1] R. Chataut, R. Phoummalayvane, and R. Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," Sensors, vol. 23, no. 16, p. 7194, 2023.

[2] H. Yar, A. B. Imran, Z. A. Khan, U. Qasim, and N. Javaid, "Towards Smart Home Automation Using IoT-Enabled Edge-Computing Paradigm," Sensors, vol. 21, no. 14, p. 4783, 2021.

[3] A. Chataut , S. K. Sharma, and S. C. Mukhopadhyay, "A Comprehensive Review of Communication Technologies for Smart Home Automation," Journal of Sensor and Actuator Networks, vol. 12, no. 2, p. 30, 2023.

[4] M. Umer, M. Sadiq, M. Ishaq, S. Ullah, A. Khelifi, and O. Strnad, "IoT Based Smart Home Automation Using Blockchain and Deep Learning," PeerJ Computer Science, vol. 9, e1304, 2023.

[5] N. K. Suryadevara, S. C. Mukhopadhyay, R. Wang, and R. Rayudu, "Smart-Home Automation Using IoT-Based Sensing and Monitoring Platform," IEEE Sensors Journal, vol. 18, no. 17, pp. 7213-7221, 2018.

[6] M. Sanjay, R. Rakshith, K. Rakshith, and K. Sumanth, "IoT Based Intelligent Home Automation Using Automated Smart Devices," in Proc. IEEE International Conference on Smart Computing, 2023.

[7] S. Ramya and B. Palaniappan, "A Smart Home Automation and Metering System Using Internet of Things," in Proc. IEEE International Conference on Communication and Signal Processing (ICCSP), 2019, pp. 0537-0541.

[8] A. Kumar, R. Sharma, and P. Singh, "IoT Based Smart Home Automation System," International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol. 11, no. 6, pp. 1-6, 2023.