International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

A Review on IoT-Based Smart Home Automation Systems

Yash H. Waghe[1], Yash A. Zade[2], Vidhan S. Shende[3]

[1, 2, 3]Electrical Engg. Dept., Govt. College of Engineering, Nagpur, Maharashtra, India

Email: [1]yashwaghe77@gmail.com, [2]yashzade22@gmail.com , [3]vidhanshende52@gmail.com

How to Cite this Article:

Waghe, Y. H., Zade, Y. A. & Shende, V. S. (2026). A Review on IoT-Based Smart Home Automation Systems. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.340

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.

https://doi.org/10.55041/ijcope.v2i4.340

Abstract—

The Internet of Things (IoT) has emerged as a transformative force in residential automation, enabling smart home systems that interconnect sensors, actuators, and computing infrastructure to deliver improved convenience, energy efficiency, and security. This paper presents a structured review of IoT-based smart home automation systems, synthesizing findings from five open-access research works covering system architectures, wireless communication protocols, hardware platforms, software frameworks, and cybersecurity. Key findings indicate that Wi-Fi and ZigBee dominate current deployments due to their complementary power and bandwidth profiles; fog computing is reshaping gateway architectures toward lower latency and greater resilience; ESP8266/ESP8285 microcontrollers and Raspberry Pi boards constitute the most widely adopted hardware platforms for cost-sensitive deployments; and cybersecurity particularly authentication, encryption, and device vulnerability management, remains the most critical unresolved challenge. Future directions including AI-driven automation, standardized interoperability, and privacy-preserving architectures are discussed.

Keywords— Internet of Things; smart home automation; Wi-Fi; wireless sensor networks.

I. INTRODUCTION

The Internet of Things (IoT) means connecting everyday devices to the internet, and many of these devices are now smart. By using embedded systems, IoT improves how we use the internet. It creates a network where devices can communicate with each other and with objects. IoT provides many opportunities to improve our daily life because of fast technology growth. With network systems, IoT helps us control different devices.

Each device connected to the internet has a unique IP address. Embedded devices are low-cost and use simple hardware with limited resources. IoT systems not only detect things but also perform tasks and follow commands. These systems are simple and need less space. It is important to keep the system flexible and secure while improving living standards. IoT home automation helps to control household devices using the internet. It can be used to create smart homes. Smart homes improve comfort, safety, convenience, and save energy. Embedded systems make it easy to create smart devices and homes. Home automation allows control of all internet-connected devices, including appliances. It is useful for elderly and disabled people, as they can easily control devices using an Android app. It also helps reduce energy usage in specific areas. Wi-Fi is now necessary in homes, making automation easier. Energy use has reduced due to automation systems, Since Wi-Fi is

affordable, it is easy to install and use. Smartphones are widely used and can connect to Wi-Fi, allowing you to control your home from anywhere in the world.

This paper reviews the current state of IoT-based smart home automation. Section II covers system architecture; Section III reviews wireless communication; Section IV discusses hardware and software platforms; Section V addresses security and privacy; Section VI presents challenges and future directions; Section VII concludes.

II. SMART HOME SYSTEM ARCHITECTURE

The architecture of IoT-based smart home systems consists of three functional tiers: the device tier, the gateway/fog tier, and the cloud tier. The device tier consists of sensors and actuators, the gateway/fog tier consists of local processing and bridging, and the cloud tier consists of remote access, storage, and analytics. This three-tier architecture strikes a balance between the conflicting demands for latency (local processing), scalability (cloud), and robustness (local intelligence) [2].

A. Device Tier

Device layer incorporates environmental sensors, temperature sensors, humidity sensors, motion sensors, illuminance sensors, air quality sensors, smoke sensors, as well as physical change actuators, switches, thermostats, doors, and appliances. As described in Stolojescu-Crisan et al. [1], the application used is qToggle, which utilizes the device layer that incorporates nodes developed based on the ESP8266/ESP8285 microcontroller platforms. This means that a central hub running on a Raspberry Pi can interact with a multitude of devices through a unified interface without using device-specific drivers.

B. Gateway and Fog Tier (Network Layer)

The gateway tier is for protocol translation, local event processing, managing the state of the devices, and providing connectivity to the cloud. Froiz-Miguez et al. [2] introduced their fog computing architecture as a Raspberry Pi-based gateway named ‘Ziwi’ to connect heterogeneous ZigBee-based sensor networks with cloud services via the WAN, utilizing the MQTT message broker as the messaging backbone.

C. Cloud Tier

The cloud tier provides remote access portals, long-term time-series storage, analytics services, and over-the-air (OTA) firmware update infrastructure. Popular cloud platforms used in smart home research and deployment include AWS IoT Core, Google Firebase, and open-source self-hosted alternatives. The dependence on cloud infrastructure introduces reliability risks, a real-world incident of service discontinuation that left functional smart home devices unable to function, which has driven interest in local-first architectures that maintain full functionality without cloud connectivity [1][2].

III. WIRELESS COMMUNICATION PROTOCOLS

Wireless communication protocols help to connect with devices wirelessly via RF signals. This also reduces power consumption and provides extended range. Table I shows the primary wireless technologies used in smart home systems.

TABLE I. Wireless Protocols Used in Smart Home Systems

Protocol	Frequency	Range	Data Rate	Topology	Power
Wi-Fi	2.4 / 5 GHz	~50 m	Up to 9.6 Gbps	Star	Med–High
ZigBee	2.4 GHz	~100 m	250 kbps	Mesh	Very Low
Z-Wave	Sub-1 GHz	~30 m	100 kbps	Mesh	Very Low
BLE 5.x	2.4 GHz	~30 m	2 Mbps	Star/Mesh	Ultra-Low
Thread	2.4 GHz	~100 m	250 kbps	Mesh (IPv6)	Very Low

A. Wi-Fi

Wi-fi is a family of wireless network protocols based on the IEEE 802.11 family of standards, which are commonly used for local area network of devices and internet access. Wi-Fi has become the dominant connectivity standard for mains-powered smart home

devices including IP cameras, smart displays, smart speakers, and set-top boxes due to its high bandwidth, ubiquitous infrastructure presence, and direct internet connectivity. Froiz-Miguez et al. [2] note, however, that Wi-Fi's relatively high energy consumption (transmit currents of 150–300 mA) and lack of native mesh networking capabilities make it poorly suited for battery-operated sensor nodes. In their Ziwi system, Wi-Fi is therefore reserved for the gateway and cloud uplink, while ZigBee handles the battery-powered sensor mesh.

B. ZigBee

ZigBee is a standard based wireless mesh network that uses a 2.4 GHz frequency band. It is primarily used for smart home automation. It supports data transfer speeds of up to 250 kbps. It consumes low power, with a current consumption of less than 1 microampere in sleep mode. This allows it to operate for more than two years on battery power. It also supports a maximum of 65,000 nodes in a single network.[2]

C. MQTT Application-Layer Protocol

MQTT (Message Queuing Telemetry Transport) is a communication protocol mainly designed for Machine-to-Machine (M2M) communication. MQTT (Message Queuing Telemetry Transport) is the dominant application-layer messaging protocol for smart home IoT, implementing a publish/subscribe model over TCP/IP via a central broker. Its minimal 2-byte fixed header, three Quality of Service (QoS) levels, and retained message capability make it highly efficient for sensor telemetry from constrained nodes. Froiz-Miguez et al. [2] deploy Eclipse Mosquitto as the MQTT broker in the Ziwi system, with ZigBee sensor readings serialized as JSON payloads and published to structured topic hierarchies. They configure Mosquitto with TLS encryption (port 8883) and username/password authentication to prevent unauthorized subscription to sensor data topics.

IV. HARDWARE AND SOFTWARE PLATFORMS

A. Microcontroller Platforms

The ESP8266 and its variant ESP8285 (Espressif Systems) are the most widely used microcontrollers in budget-oriented smart home research, integrating a 32-bit Tensilica L106 core with 802.11b/g/n Wi-Fi at a retail price below USD 2. Both Froiz-Miguez et al. [2] and Stolojescu-Crisan et al. [1] employ these SoCs as sensor and actuator node platforms. Stolojescu-Crisan et al. [1] specifically adopt the NodeMCU development board (based on ESP8266) for its low cost (approximately USD 4), ability to interface with 5 V sensors and actuators, and support for development in both Lua and C via the Arduino IDE. The successor ESP32 adds dual-core Tensilica LX6 processing, Bluetooth 4.2/BLE, hardware AES acceleration, and improved power management, making it preferable for applications requiring greater computational capability or cryptographic security.

B. Single-Board Computers and Gateways

Raspberry Pi single-board computers are widely adopted as smart home gateway and hub hardware due to their full Linux operating system support, GPIO and multi-interface connectivity, and active open-source ecosystem. In both reviewed systems [1][2], the Raspberry Pi serves as the central hub, running gateway middleware, MQTT brokers, and dashboard software. For security-critical gateway applications, Abu-Tair et al. [3] evaluate lightweight symmetric cryptographic algorithms on ARM Cortex-A series platforms, finding that algorithms such as CLEFIA and TRIVIUM, despite being optimized for hardware, can consume up to 10× more energy than legacy AES when implemented in software on commodity gateway hardware, an important practical consideration for energy-efficient secure gateway design.

C. Software Middleware

Open-source middleware platforms provide the software backbone for home automation. The qToggle system [1] implements a custom RESTful API allowing each device to self-describe its capabilities, enabling plug-and-play integration of new devices without per-device driver development. Froiz-Miguez et al. [2] use a layered fog stack comprising TI Z-Stack ZigBee coordinator firmware, a Python-based ZigBee-to-MQTT translation gateway, Eclipse Mosquitto broker, and a Node.js web dashboard for real-time visualization. These complementary approaches demonstrate two viable middleware philosophies: a unified API abstraction layer [1], and a protocol translation pipeline built on standard messaging infrastructure [2].

V. SECURITY AND PRIVACY

Security and privacy are the most critical and persistently challenging aspects of IoT smart home deployment. The convergence of digital control with physical systems creates novel attack surfaces: a compromised smart lock enables physical intrusion, a hijacked camera violates personal privacy, and a hacked appliance controller can cause property damage. Abu-Tair et al. [3] provide a comprehensive examination of this threat landscape and propose a layered security architecture specifically designed for constrained IoT smart home devices.

A. Threat Categories

Abu-Tair et al. [3] categorize smart home security threats across four layers: the perception layer (physical tampering, sensor spoofing, node capture), the network layer (eavesdropping, man-in-the-middle, replay attacks), the middleware layer (unauthorized API access, session hijacking), and the application layer (data poisoning, privacy inference from behavioral data). They emphasize that the constrained nature of IoT sensor nodes, limited RAM, CPU, and battery, severely restricts which cryptographic mechanisms can be practically deployed, creating a fundamental tension between security strength and resource efficiency. Nemec Zlatolas et al. [4] add a user-behavior dimension, reporting from a 306-participant survey that user awareness of specific threats, data breaches, ransomware, personal information access violations, and device vulnerabilities, significantly influences perceived IoT security importance, suggesting that user education is as important as technical countermeasures.

B. Encryption and Authentication

Abu-Tair et al. [3] experimentally evaluate multiple lightweight cryptographic algorithms for securing constrained IoT smart home nodes, finding that modern lightweight symmetric ciphers designed for hardware implementation (CLEFIA, TRIVIUM) are unsuitable for software deployment on typical IoT microcontrollers due to excessive energy consumption. They recommend AES-128 in CCM mode as the best balance of security strength and software efficiency for resource-constrained nodes, which aligns with the encryption model used in the ZigBee security sublayer. For gateway-to-cloud links, TLS 1.3 with certificate-based authentication is the recommended standard. Froiz-Miguez et al. [2] implement TLS on the MQTT broker interface and username/password device authentication in their Ziwi system as pragmatic measures, while acknowledging that certificate lifecycle management across large heterogeneous device fleets remains operationally challenging.

C. Privacy Considerations

Smart home sensor streams constitute highly sensitive personal data, environmental sensor patterns reveal occupancy schedules and daily routines, audio streams may capture private conversations, and video feeds enable real-time surveillance. Abu-Tair et al. [3] recommend a data minimization architecture in which raw sensor data is processed locally at the fog gateway tier, with only derived events or aggregated statistics transmitted to the cloud, directly reducing the volume of sensitive data exposed to external services. The EU General Data Protection Regulation (GDPR) and India's Personal Data Protection Bill impose data minimization, purpose limitation, and breach notification requirements on smart home service providers that reinforce this architectural approach. Nemec Zlatolas et al. [4] find that user awareness of data collection practices significantly affects adoption intent, underscoring the importance of transparent privacy policies and user-facing data controls.

VI. CHALLENGES AND FUTURE DIRECTIONS

A. Interoperability

Device interoperability remains the most persistent structural challenge in smart home IoT. Even when devices share a common wireless protocol such as ZigBee or Wi-Fi, differences in application-layer data models, control semantics, and cloud ecosystems prevent seamless multi-vendor integration. Stolojescu-Crisan et al. [1] partially address this at the device level through a standardized qToggle API that enables protocol-agnostic device management, but acknowledge that cross-ecosystem integration at the cloud and voice-control layers requires additional bridging. The Matter protocol (CSA, 2022), not yet widely deployed at the time of the reviewed papers, represents the most significant recent industry effort to address application-layer interoperability by defining a unified device model operable over Wi-Fi, Thread, and Ethernet.

B. Security Scalability

While individual security mechanisms have been demonstrated for smart home IoT, their consistent and scalable deployment across heterogeneous device fleets remains an open problem. Abu-Tair et al. [3] identify device heterogeneity, spanning highly constrained sensor nodes and capable gateway hardware, as the primary obstacle: a one-size-fits-all security approach is infeasible given the orders-of-magnitude variation in computational and energy resources. Automated certificate provisioning, lightweight attestation protocols, and hardware security elements (e.g., ATECC608B secure microchip) are emerging solutions, but their integration into mass-market smart home products remains limited. Nemec Zlatolas et al. [4] further highlight that low user awareness and complexity of security configuration create a human-factors barrier that technical solutions alone cannot overcome.

C. Cloud Dependency and Resilience

Cloud-dependent smart home architectures create single points of failure. The shutdown of multiple commercial smart home cloud services in recent years rendered thousands of functional devices inoperable, demonstrating that cloud dependency is a practical resilience risk, not merely a theoretical concern. The fog-computing architecture of Froiz-Miguez et al. [2] and the local-API approach of Stolojescu-Crisan et al. [1] both provide partial solutions by enabling continued local control during WAN outages. Building on this, future research should formalize resilience requirements for smart home systems, including maximum tolerable cloud unavailability periods and mandatory local fallback operation modes.

D. Artificial Intelligence Integration

The reviewed literature focuses primarily on connectivity and basic automation. The integration of machine learning and AI into smart home systems represents the most significant near-term growth area. Key application domains include occupancy and activity recognition from multi-sensor fusion data, reinforcement learning-based HVAC and energy optimization, non-intrusive load monitoring (NILM) for per-appliance energy disaggregation, and large language model-based natural language interfaces for accessible automation programming. Privacy-preserving approaches such as federated learning, training models across devices without centralizing raw data, are particularly promising for cross-home intelligence that respects GDPR-class data protection requirements [3][4].

VII. CONCLUSION

This paper has reviewed IoT-based smart home automation systems through the lens of five open-access research contributions covering architecture, protocols, hardware, software, and security. The qToggle system [1] and the Ziwi fog-computing platform [2] demonstrate two practically implemented and experimentally validated architectures that span the design space from unified API abstraction to protocol-bridging fog gateways. Both confirm the dominance of ESP8266/ESP8285 microcontrollers and Raspberry Pi gateways as the de facto hardware baseline for cost-effective smart home research prototypes.

The reviewed works collectively establish that Wi-Fi and ZigBee are complementary rather than competing technologies, with Wi-Fi suited to high-bandwidth mains-powered devices and ZigBee suited to low-power battery-operated sensor nodes. MQTT over TLS is the recommended application-layer protocol stack. Security, analyzed in depth by Abu-Tair et al. [3] and from a user-perspective by Nemec Zlatolas et al. [4], remains the most critical unresolved challenge, requiring progress in lightweight cryptography deployment, automated certificate management, and user security awareness.

Future work should prioritize standardized interoperability frameworks, AI-driven context-aware automation, privacy-preserving federated learning, and formally specified resilience requirements for local operation independence. With these advances, IoT-based smart home systems are well-positioned to deliver meaningful improvements in residential energy efficiency, comfort, security, and quality of life.

Highlight the significance of your contribution and suggest areas for future work. Avoid repeating sentences from the abstract.

REFERENCES

[1] C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, "An IoT-Based Smart Home Automation System," Sensors, vol. 21, no. 11, Art. 3784, May 2021. DOI: 10.3390/s21113784.

[2] I. Froiz-Miguez, T. M. Fernandez-Carames, P. Fraga-Lamas, and L. Castedo, "Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes," Sensors, vol. 18, no. 8, Art. 2660, Aug. 2018. DOI: 10.3390/s18082660.

[3] M. Abu-Tair, S. Djahel, P. Perry, B. Scotney, U. Zia, J. M. Carracedo, and A. Sajjad, "Towards Secure and Privacy-Preserving IoT Enabled Smart Home: Architecture and Experimental Study," Sensors, vol. 20, no. 21, Art. 6131, Oct. 2020. DOI: 10.3390/s20216131.

[4] L. Nemec Zlatolas, N. Feher, and M. Holbl, "Security Perception of IoT Devices in Smart Homes," J. Cybersecur. Priv., vol. 2, no. 1, pp. 65-73, Feb. 2022. DOI: 10.3390/jcp2010005.]

[5] G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Taur, and E. Ayday, "A survey on information security threats and solutions for Machine to Machine (M2M) communications," J. Parallel Distrib. Comput., vol. 109, pp. 142-154, 2017. DOI: 10.1016/j.jpdc.2017.05.021