Proceedings of CONF-MLA 2026 Symposium: Intelligent Systems and Automation: AI, IoT, Robotic Engineering & Algorithm
DOI: 10.54254/2755-2721/2026.LD35654

Smart Home IoT: Current Development, Bottlenecks, and Optimization Strategies

Haoxiang Shi

The School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China
shx18101480227@my.swjtu.edu.cn

Abstract. The Internet of Things (IoT) and artificial intelligence have advanced quickly, and with shifting consumer behaviors, the smart home has become the most promising field of IoT application. Rapid growth, however, has exposed persistent weaknesses in interoperability, security, and reliability that slow adoption. This paper analyses the deployment of smart home IoT and the obstacles it faces. The paper first clarifies the concept of the smart home and its underlying IoT infrastructure, then reviews the industry's evolution, and finally assesses the domestic market from four angles: overall scale, penetration rate, major platforms and ecosystems, and typical application scenarios. It then identifies five recurring problems—limited interoperability and ecosystem fragmentation, security and privacy hazards, conflicting automation logic and unreliable operation, a weak user experience, and high cost and energy use alongside lagging standards—and proposes strategies built around unified standards, security-oriented design, conflict detection and mitigation, edge computing with AI, and aging-friendly design. Methodologically, the study combines literature review, case analysis, and industry statistics. It concludes that China's smart home market, though large and fast-growing, remains in a growth phase, and that its tensions are best resolved through stronger standards, a security-first stance, and a systems perspective. Finally, since closed commercial ecosystems provide no usable means of detecting rule conflicts, the study put forward a black-box, log-driven approach to conflict identification and severity assessment that requires neither platform source code nor proprietary interfaces. Unlike techniques that depend on open APIs or runtime instrumentation, it can inform risk governance in multi-brand smart homes and the drafting of technical standards.

Keywords: smart home, Internet of Things, adoption status, rule conflicts, security and privacy

1. Introduction

Advances in IoT, cloud computing, and artificial intelligence over the past decade have made device connectivity and intelligent control far more feasible, laying the technical groundwork for large-scale smart home deployment. At the same time, rising incomes and growing demand for secure, convenient, energy-efficient, and comfortable housing have brought smart security, lighting, and appliances into ordinary households.

DOI: 10.54254/2755-2721/2026.LD35654

Academic work on smart homes has concentrated on technical security. From a systems-security perspective, Celik et al. proposed Soteria and IoTGuard, which analyze the safety of automation applications statically and at runtime respectively [1, 2]; Wang et al. exposed vulnerabilities in trigger-action platforms [3]; and Ding et al. drew on real physical interactions to strengthen system security [4]. Surveys have mapped privacy and security difficulties through a layered, IoT-oriented lens [5, 6]. Such work centers on technical mechanisms or vulnerabilities and rarely engages with how these technologies are taking root in the domestic industry. Industry reports, conversely, size the market and describe its landscape, but seldom address the structural tensions underlying adoption. No study has yet combined domestic penetration, usage patterns, and the principal problems into a single framework—precisely the gap this paper addresses.

The discussion concentrates on the domestic market and follows a logical progression from concept to status, then to problems and solutions, drawing on literature review, case study, and statistical methods. It first clarifies the notion of smart home IoT and its developmental stages, then reviews the market, the principal ecosystems, the evolution of usage, and concrete cases, before turning to today's chief difficulties and to suggestions for improvement. In doing so, the study helps redress a research imbalance that has favored technical mechanisms over the realities of domestic deployment, and provides localized guidance for setting industry standards, designing cross-ecosystem interoperability, and optimizing products for elderly users.

2. Definition of smart home IoT

A smart home is a residence-based system that uses communication, automatic control, and sensing technologies to link household facilities—lighting, appliances, security, audio-video equipment, environmental controls—and manage them centrally or automatically, giving occupants a safe, convenient, comfortable, and energy-efficient environment. Early implementations relied on wired and timer-based control, emphasizing remote operation and scheduling.

The IoT endows physical objects with the ability to perceive, connect, and process data. Smart home IoT is IoT applied in the residential setting: device networking, real-time data requirements, and the cloud–edge division of labor are designed around household needs, while rule-based logic and AI drive automated decision-making. Traditional smart homes focus on whether centralized control is feasible; smart home IoT emphasizes connectivity, perception, and autonomy, so that a device no longer merely obeys commands but senses, relays information, and acts on the user's behalf—functioning, in effect, as an agent.

The development of smart home IoT can be divided into three phases. In single-product intelligence, one connected device—Xiaomi's smart speakers or door locks, say—handles a specific task alone. In interconnection, devices of various categories are coordinated through a unified app and a central gateway, for example, when the Mi Home and Huawei AI Life apps drive lighting, climate control, and curtains in concert through scenes such as "coming home" and "bedtime." In whole-home intelligence, up-front design, integration, and proactive service are combined, and AI such as large language models increasingly enables more proactive and less obtrusive interaction;; Huawei's HarmonyOS-based "1+8+N" solution, Haier's Three-Winged Bird approach, and Midea's MSmart package are representative. China is currently in transition from the second phase to the third.

DOI: 10.54254/2755-2721/2026.LD35654

3. Market uptake and usage models of smart home IoT

3.1. Penetration of the domestic market

China's smart home market has expanded steadily. Industry researchers estimated its value at about 651.6 billion yuan in 2022 and 715.7 billion in 2023, and expect 785–800 billion across 2024–2025, a rate that remains essentially in double digits; by 2024, market penetrationhad reached roughly 21% of households, with device shipments up almost 6.5% year on year [7]. Smart appliances are the largest segment, while connectivity, security, lighting, and energy management together account for less than a fifth [7].

These figures repay closer reading. First, growth has cooled: the near-double-digit surge of 2022–2023 has given way to a band of single to low double digits, indicating that the sector is transitioning from high-speed expansion to a growth phase shaped by structural adjustment. Second, the 21% coverage comes overwhelmingly from first-, second-, and new first-tier cities; in lower-tier markets, where income, network conditions, and buying habits weigh against it, penetration is visibly thinner, which constitutes the chief drag on further uptake. Third, the dominance of smart appliances shows that growth springs more from making individual appliances smarter than from knitting devices together across categories, an early demand-side sign of the ecosystem fragmentation discussed below.

The industry chain has coalesced into a rough loop—chips, sensors, and modules upstream; manufacturing and platforms midstream; sales and after-sales downstream—though high-end chips and sensors still rely heavily on foreign suppliers.

3.2. Comparison of leading ecosystems and platforms

China's smart home market is organized around two rival platform ecosystems. The first is internet and technology brands: Xiaomi has risen fast on keen pricing and an open Mi Home ecosystem, while Huawei rests connectivity on HarmonyOS together with HiLink and NearLink, using a distributed design to bring disparate devices under one roof. The second is the old-line appliance makers—Haier and Midea—whose strengths lie in manufacturing, quality, and offline service. Each camp has its edge, but each operates with proprietary protocols, leading to fragmentation.Table 1 compares the four leading ecosystems. Each has its own mature technical route and target audience, yet all share a similar inclination—favoring proprietary protocols over cross-vendor interoperability. Matter has taken off abroad, but the domestic mainstream has held it at a distance, only a few peripheral products attempting support. That shared blind spot is the backdrop against which the interoperability problem unfolds.

Table 1. Comparison of the leading domestic smart home ecosystem platforms

Dimension	Xiaomi Mi Home (MIoT)	HarmonyOS / HiLink / NearLink	Haier Smart Home	Midea MSmart
Connectivity protocols	Wi-Fi, Bluetooth Mesh, Zigbee; multi-mode gateway bridges protocols	HarmonyOS soft bus; NearLink; PLC	U+ IoT platform; multi-protocol gateways	Bluetooth Mesh, Wi-Fi, NearLink; local scene linkage
Ecosystem openness	High: 300+ chain firms; 600M+ devices	Medium: 2,000+ HarmonyOS Connect brands; app-free control Huawei-only	Medium-low: own lineup + ~20,000 partners	Medium: full lineup; tied in with HarmonyOS

DOI: 10.54254/2755-2721/2026.LD35654

Table 1. (continued)

Core strengths	Largest device range; user-defined "if-then" rules; low entry cost	Seamless cross-device handoff; deep sensor coverage; reliable linkage	Full-category depth; pre-installation engineering; offline service; scene customisation	In-house lineup enables deep linkage; proactive scenarios at scale
Core weaknesses	Uneven hardware quality; software integration lags	Little value outside the Huawei fold	AI capability and openness lag; package price high	Weaker standalone ecosystem; non-Midea support immature
Matter adoption	Cautious; a few peripheral devices only	Not at scale; prefers HarmonyOS Connect / NearLink	On the sidelines; no broad interconnection	CSA member, but not yet a priority
Target users	Cost-conscious DIY young tech users; Xiaomi phone owners	Huawei device users; upper-middle households valuing system-level connectivity	Upper-middle pre-installation buyers; existing Haier owners	Households wanting one-stop proactive service; existing Midea owners

3.3. Evolution of smart home application modes

Usage has followed the same three stages: isolated single products; rudimentary linkage, in which an app and a central gateway coordinate devices within one ecosystem through scenes; and whole-home intelligence, in which design and wiring are determined at the renovation stage, subsystems are integrated onto one platform, and AI drives sensing and service. Interactionevolves accordingly—from app taps and voice commands to rule-driven and, in time, AI-led service, so the home shifts from something you control to something that acts for you.

3.4. Typical real-world application scenarios

Smart home IoT has landed in several settings. In private homes—by far the commonest use—smart security (cameras, locks), lighting, appliances, and audio-video anchor the setup. In commercial venues, smart hotels offer one-touch control of lights, curtains, air conditioning, and audio-video, while long-stay rentals rely on smart locks and utility meters to operate without on-site staff.

The third setting is elderly care, propelled by both policy and need. By the close of 2024 China had 310 million people aged 60 or older, 22.0% of the population [8]. Measures such as the Guidelines on Developing the Silver Economy are vigorously promoting aging-friendly smart homes; centered on basic safety and health management, their penetration rose from roughly 3.5% in 2020 to about 12% in 2024 [9]. Fall detection, health monitoring, emergency calls, and remote care are catching on fast.

The practical difficulties are equally real. Pairing and scene setup are still built around younger users, and over half of older users have dropped features they found too hard to work [9]; if fall detection or an emergency call drops out over a shaky network, help can come too late; and some older people, uneasy about cameras and vital-sign monitors, decline to use them on privacy grounds [9]. Aging-friendly design must thereforevigorously promoting aging-friendly smart homes;to ease of use and to earning trust.

DOI: 10.54254/2755-2721/2026.LD35654

4. Pressing problems in today's smart home IoT systems

4.1. Weak interoperability and a fractured ecosystem

Interoperability is among the plainer structural faults. The big vendors have long kept to separate protocols and walled gardens—Huawei HiLink, Xiaomi MIoT, Haier Smart Home—so devices from different makers cannot easily interoperate, and data silos result. Put several brands under one roof and endless app-hopping breaks the user's stride while the linkages on offer come up short. Matter has made headway [10] and sketches a unified interoperability scheme at the application layer, yet the difficulty of updating installed equipment, together with ecosystem lock-in, means full interconnection remains distant.

4.2. Security and privacy risks

Smart homes now contain many kinds of device whose firmware and safeguards often have shortcomings; some cut-price products ship flawed, easy prey for unauthorized access, hijacking, or network attacks [5, 6]. Privacy deserves particular attention: cameras and voice devices capture a household's talk, movements, even physical states, yet that information can go under-protected at capture, upload, storage, and sharing.

Real incidents bear this out. For instance, EZVIZ Cloud was found in 2021 to carry a flaw that let users pull up live camera feeds from other properties, while a system fault at Wyze left some 13,000 users looking at strangers' footage. On hijacking, researchers showed at Def Con 2024 that Ecovacs robot vacuums could be turned into surveillance tools through their cameras and microphones, and police in Jiangsu busted a ring that had reflashed close to 4,000 smart refrigerators into mining rigs. Both undermine users' sense of safety and trust, and therefore stand out as a leading barrier to adoption.

4.3. Automation rule conflicts and reliability

Households now have so many automation rules that the linking logic conflicts with itself, dragging reliability down. Conflicts fall into three kinds.

Command conflict arises when two rules issue opposed orders to the same actuator: a "coming home" scene wants the living-room light on while an "unoccupied energy-saving" scene, reading no motion, wants it off, so the lamp flickers or stays in an indeterminate state.

Physically mediated conflict arises when rules do not contend for the same device but push against one another through a shared physical quantity: a heating rule starts an electric heater because the room is cold while a ventilation rule opens a window because the air is stale, and by way of room temperature the two keep counteracting and re-triggering, wasting energy without reaching stability.

Cross-ecosystem linkage conflict crops up when devices from different brands are pulled into one scene but their rules cannot coordinate with each other. A Xiaomi thermostat and a Huawei curtain and air conditioner live in separate apps, so on a summer day "draw the curtains to shade the room" and "open the window to air it out" can fire together with nothing coordinating them. Once several ecosystems coexist, this kind is the commonest and the hardest to catch.

Existing detection work—Soteria, IoTGuard—depends on platforms providing source code, runtime hooks, or bespoke interfaces; since commercial systems from Xiaomi, Google, and Amazon do not disclose these, most users are left with no method they can actually use [1, 2].

DOI: 10.54254/2755-2721/2026.LD35654

4.4. User-experience problems

A rough user experience is a real brake on adoption. Network pairing, binding, and scene arrangement are not intuitive to understand, and for older people new to smart gear they area considerable barrier; in daily use, wobbly networks, uncooperative devices, and laggy voice feedback make the promise of "works the moment you buy it" fall flat. The shelves are crowded, too, with pseudo-smart goods that offer little beyond app-based remote control, so satisfaction and the appetite to keep going both fade.

The shortfall is most acute in aging-friendly settings, where simplicity and reliability are paramount. Tangled pairing routines, interfaces pitched at younger habits, and flaky voice recognition leave many older users unable to manage the basics alone. Polishing the experience cannot be limited to features: it must clearly articulate aging-friendly objectives—getting it right on the first attempt, allowing recovery from failures, and providing readable feedback.

4.5. High cost and energy use, and lagging standards

Whole-home intelligence involves design, wiring, device fit-out, and often building work, which can be costly; top-tier schemes cost too much and retrofitting is awkward, so they have limited penetration in mid-range and lower-tier markets.

Running many connected devices also mounts up into a hefty energy load. To stay online and ready to answer, devices remain on standby for long stretches; with a single smart speaker, set-top box, or optical modem typically pulling 1 to 10 watts and a mid-sized whole-home build hooking up dozens at a time, the standby draw compounds into a hidden electricity bill. Set against the national dual-carbon push, this load pulls against the low-carbon line; without energy-saving design and unified consumption management, a smart home may in fact goad household energy use upward.

On the regulatory front, laws covering device interoperability and the handling of security and data remain incomplete, and standards have not kept up with how fast the products have spread.

5. Strategies for improving smart home IoT systems

5.1. Unified standards and interoperability

Untangling the fractured ecosystem has to start with unified standards. At industry level, multi-vendor interconnection schemes such as Matter or Thread ought to be adopted or co-developed, providing a shared interoperability language at the application and network layers. At company level, firms should open their interfaces and APIs in a measured way, so that devices of different brands can recognize and work with one another, installed equipment included. Loosening ecosystem lock-in serves users and the market alike.

5.2. Security and privacy protection

Security and privacy must be considered throughout a device's whole life. For security: end-to-end encryption, device identity checks, access control (least privilege and zero trust), and prompt vulnerability disclosure and patching. For privacy: privacy-first design—gather as little data as possible, keep sensitive household audio and video to local or edge processing, and hold privacy terms open and in the user's hands. Behavioral baselines can flag anomalies early, catching a hijacked device before it does harm [11].

DOI: 10.54254/2755-2721/2026.LD35654

5.3. Rule conflict detection and severity assessment

Because closed commercial platforms offer no way to detect conflicts, this paper proposes a black-box, log-driven approach. Timestamped device logs, which platforms can generally export, serve as the raw data; time windows tie the data together and work backward to the rules behind the automation. Causal links picked up passively from the logs then separate physically direct conflicts from indirect ones, taking care not to mistake coincidence for interference. Conflicts are then ranked by risk against a severity yardstick, sizing up harm with reference to established safety gradings and setting weights by the analytic hierarchy process.

Because none of this requires access to a platform's internal code, it can work through a large batch of commercial residential cases at once and return conclusions that are explained and ordered by risk.

5.4. Edge computing and an AI boost

Pushing inference and its rules down to the home gateway or the edge shortens response times, handles cloud outages more gracefully, and transmits less sensitive data—addressing efficiency and privacy in one stroke. Bringing in AI at that point, whether an on-device small model or a large language model, offers grounding for situational judgement and a natural, interactive mode of interaction; it can also learn a household's rhythms to help with monitoring, energy saving, and device-state forecasting, moving the home from a system that reacts to one that acts proactively.

5.5. Better user experience

Products should be designed around the value of real scenarios and steady long-run operation, not sheer feature count.In practice, this translates into simple pairing, plug-and-play self-recognizing devices, and operations that are as straightforward as possible, with particular attention to the elderly and less mobile users; more reliable and faster linkages, with transparent automation that explains to users why a particular action was triggered; and pricing structured at the single-item, bundle, and whole-home levels.

6. Conclusion

With the domestic market as its anchor, this paper has examined the development, bottlenecks, and improvement strategies of smart home IoT. China's market is large and fast-moving, with internet firms and old-line appliance makers both entering the contest; usage is shifting from single-product intelligence toward integrated whole-home intelligence, and deployments already dot private homes, commercial venues, and elderly-care facilities—though by penetration and product mix the industry is still in a developmental phase. Five bottlenecks stand out: weak interoperability and a fractured ecosystem, security and privacy risks, automation rule conflicts and compromised reliability, an unsatisfactory user experience, and high cost and energy use alongside lagging standards. Each is bound up with the others, and together they hold smart homes back from transitioning from merely usable to genuinely pleasant to use. The paper accordingly puts forward a joined-up response: unified standards to break the fragmentation, whole-life-cycle security and privacy protection to rebuild trust, conflict detection and severity assessment to shore up reliability, edge computing and AI to power proactive service, and aging-friendly design to lift the user experience.

DOI: 10.54254/2755-2721/2026.LD35654

Where the paper breaks new ground is in tackling a plain reality: closed platforms keep source code and proprietary interfaces to themselves, leaving existing detection methods with nowhere to land. Its black-box, log-driven scheme reconstructs automation rules from timestamped logs, identifies physically mediated conflicts by time-window correlation and causal inference, and ranks them by risk—a workable route to risk governance under closed ecosystems.

The study has limits: it relies on literature, statistics, and cases rather than large-scale household measurements, and the scheme awaits a prototype. Future work should build and test that prototype, integrate on-device small models with large language models for proactive human–machine collaboration, and promote localized standards for aging-friendliness, energy management, and data compliance.

References

[1] Celik, Z. B., McDaniel, P., & Tan, G. (2018). Soteria: Automated IoT safety and security analysis. *Proceedings of the USENIX Annual Technical Conference (USENIX ATC)*, Boston, MA, 147-158.

[2] Celik, Z. B., Tan, G., & McDaniel, P. (2019). IoTGuard: Dynamic enforcement of security and safety policy in commodity IoT. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA.

[3] Wang, Q., Datta, P., Yang, W., Liu, S., Bates, A., & Gunter, C. A. (2019). Charting the attack surface of trigger-action IoT platforms. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, London, UK, 1439-1453.

[4] Ding, W., Hu, H., & Cheng, L. (2021). IoTSafe: Enforcing safety and security policy with real IoT physical interaction discovery. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

[5] Zia, M. F., Siddiqua, M., Ouameur, M. A., Bagaa, M., & Al Turjman, F. (2025). Securing the future: A survey on smart home security in IoT-integrated smart cities. *Advances in Networks, 12*(1), 1-18.

[6] Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: Challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing, 77*, 14053-14089.

[7] China Business Industry Research Institute (CSHIA). (2025). A survey of China's smart home industry chain, of its size and of competition (for years 2024-2025) [Industry report] (in Chinese).

[8] National Bureau of Statistics of China. (2025). Statistical communique of the People's Republic of China on the 2024 national economic and social development (in Chinese).

[9] LeadLeo Research Institute. (2025). White paper about China's smart elderly-care items 2025 [Industry report] (in Chinese).

[10] Connectivity Standards Alliance. (2024). Matter specification. Retrieved from https://csa-iot.org/all-solutions/matter/

[11] Fu, C., Zeng, Q., & Du, X. (2021). HAWatcher: Semantics-aware anomaly detection for appified smart homes. *Proceedings of the 30th USENIX Security Symposium*, 4223-4240.