I.J. Information Engineering and Electronic Business, **2026, 3, 185-202**
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2026.03.11

IoT-Based Smart Homes: Technologies, Security Risks and Countermeasures

Tanvir Ahmed
Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh
E-mail: 2001028@iot.uftb.ac.bd
ORCID iD: https://orcid.org/0009-0002-5760-3198

Akhterujjaman Siddiquee
Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh
E-mail: 2001031@iot.uftb.ac.bd
ORCID iD: https://orcid.org/0009-0002-0260-4409

Sheikh Sidratul Muntaha Punno
Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh
E-mail: 2001047@iot.uftb.ac.bd
ORCID iD: https://orcid.org/0009-0003-3288-3063

Md. Moshiur Rahman
Department of Software Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh
E-mail: moshiur0001@uftb.ac.bd
ORCID iD: https://orcid.org/0000-0002-0279-0793

Fahmida Ahmed Antara
Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh
E-mail: fahmida0001@uftb.ac.bd
ORCID iD: https://orcid.org/0009-0003-0005-1510

Sadia Enam*
Department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh, Gazipur, 1750, Bangladesh
E-mail: sadia0001@uftb.ac.bd
ORCID iD: https://orcid.org/0009-0001-3424-8042
*Corresponding author

Received: October 2, 2025; Revised: December 19, 2025; Accepted: February 2, 2026; Published: June 8, 2026

Abstract: The advent of Internet of Things (IoT) technologies has essentially transformed traditional houses into intelligent, equipped, and networked smart houses that serve to improve the quality of life of human beings with respect to security, energy efficiency, and comfort through massive automation, sensing, and remote control. However, such a shift of paradigm, due to the diversity of devices, the limitation of resources, problems of interoperability, and a growing array of cyberthreats, opens up numerous avenues for security and privacy threats. This review attempts a holistic coverage of IoT-based smart home technologies and then provides a systematic classification of the security vulnerabilities from device, network, cloud, and application layers. The key threats include unauthorized access, data leakage, propagation of malware, denial of service, and exploits targeted against AI, with an analysis of their causes and occurrences in the real world. The paper undertakes a critical assessment of contemporary countermeasures, ranging from lightweight cryptographic protocols, AI-driven intrusion detection systems, blockchain-based authentication, privacy-preserving edge computing, and zero-trust frameworks. A comparative insight into each approach compared with the views of the established literature draws out trade-offs between security efficacy, scalability, computational

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

overheads, and user adoption. Based on a synthesis of the modern findings, continued gaps are identified, and future directions provided, including quantum-resistant encryption, interoperable standards, and user-centric security design, acting as the working platform or actionable directions for any researchers, developers, or policymakers in building a secure, resilient, and privacy-preserving smart home ecosystem.

Index Terms: Internet of Things, Smart Homes, Cybersecurity, Privacy, Intrusion Detection, Blockchain, Edge Computing, IoT Technologies

1. Introduction

An Internet of Things (IoT)–based paradigm has rapidly transformed the traditional structure of residential life by making homes intelligent, connected, and automated. The combination of pervasive sensing, embedded systems, cloud computing, and wireless communication has given rise to smart homes, residential environments that deliver comfort, energy efficiency, security, and personalization through intelligent automation and remote control of household systems. IoT-based smart homes are gaining traction worldwide, driven by consumer demand, decreasing hardware costs, and advances in automation platforms [1]. At the same time, surveys highlight that while convenience and energy efficiency are strong adoption drivers, concerns about privacy, interoperability, and reliability remain key barriers [2].

As the diversity of interconnected devices increases, complex security and privacy challenges emerge across heterogeneous hardware, communication protocols, and vendor ecosystems. Empirical measurement studies demonstrate that even encrypted smart-home traffic can leak sensitive information about user activities, enabling behavioral inference, profiling, and surveillance through traffic pattern analysis [3]. Protocol-level studies reveal exploitable weaknesses in wireless IoT standards such as Zigbee, Z-Wave, and Thread, which underpin smart-home ecosystems [4]. Experimental investigations into intrusion detection also demonstrate that while tools such as Snort, Suricata, and Bro can be applied to smart-home traffic, their effectiveness varies depending on configuration and resource constraints [5]. In addition, forensic analyses emphasize that IoT systems often lack robust investigation frameworks, making it difficult to ensure accountability in the event of compromise [6].

A wide spectrum of countermeasures has been proposed to address these risks. Lightweight cryptographic methods are emphasized as a means of protecting constrained devices while minimizing performance overheads [6]. Blockchain-based frameworks are increasingly studied as decentralized solutions for authentication, trust management, and tamperproof storage [7]. Forensic-ready architectures combine blockchain with IoT evidence preservation to support transparent investigation processes [8]. Recent advances also explore quantum-resilient security mechanisms, such as post-quantum blockchain over NTRU lattices and quantum-assisted blockchain using quantum signatures, to safeguard smart homes against future quantum adversaries [9]. Complementary work proposes multi-layered quantum-resilient IoT architectures that integrate relativistic blockchain and decentralized storage for long-term security [10]. Collectively, these directions illustrate a strong momentum toward integrating security-by-design into smart-home ecosystems, though challenges of scalability, energy efficiency, and cross-vendor interoperability remain unresolved [11].

With expectations rising for systems that are not only functional but also secure-by-default and user-centric, the future of smart home security demands solutions that are adaptive, scalable, and usability-driven. Emerging surveys emphasize that combining technical safeguards with usability and governance frameworks will be essential to building long-term user trust in IoT-enabled residential environments [1]. This review paper aims:

- To provide a comprehensive overview of IoT-based smart home technologies, highlighting their architectural foundations, components, and interaction paradigms.
- To systematically categorize security threats and vulnerabilities across device, network, cloud, and application/AI layers.
- To critically examine existing countermeasures, including lightweight cryptographic protocols, intrusion detection systems, blockchain-based frameworks, and privacy-preserving approaches, with attention to their trade-offs.
- To identify gaps and future research needs for building secure, resilient, and privacy-preserving smart home ecosystems.

In order to provide systematic guidance for this review, the following research questions have been developed. These enquiries offer the structure for examining the technical underpinnings, identifying weaknesses, and assessing defences in Internet of Things-based smart homes.

- RQ1. What are the key technological enablers of IoT-based smart homes, and how do they interact to support automation, security, and user experience?
- RQ2. Which security vulnerabilities most significantly impact smart home environments across device,

network, cloud, and application layers?

- RQ3. How effective are the countermeasures and frameworks in addressing the unique constraints of resource-constrained smart home systems?
- RQ4. Where do gaps remain, and what future directions are most critical for advancing secure smart home deployments?

The remainder of this paper is organized as follows: Section 2 presents the methodology, Section 3 provides the background, motivation, and an overview of IoT-based smart homes. Section 4 discusses the core IoT technologies that enable smart homes, including sensors, controllers, communication protocols, and AI integration. Section 5 systematically reviews the security risks and threat landscape across device, network, cloud, and application layers. Section 6 examines existing countermeasures and security mechanisms such as lightweight cryptography, IDS, blockchain, and edge computing. Section 7 presents a comparative analysis and discussion of the strengths, weaknesses, and trade-offs of current approaches. Section 8 outlines open challenges and future research directions. Section 9 discusses the answers to the research questions, Section 10 provides the overall discussion of this study, and finally Section 11 concludes the paper with key findings and implications.

2. Methodology

This paper utilizes a systematic literature review process to explore the technological underpinnings, security issues and mitigation strategies of IoT-based smart homes. To facilitate the presentation of the review, four research questions are employed, which cover (i) the major technological enablers and interaction, (ii) security vulnerabilities between architectural layers, (iii) the effectiveness of current countermeasures in the face of resource constraints, and (iv) the research gaps and the way forward.

It was a systematic search that was performed in compliance with the PRISMA (Preferred Reporting Items to Systematic Reviews and Meta-Analyses) guidelines. Peer-reviewed journal and conference articles published between 2015 and 2025, mostly from major academic databases, such as IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier, MDPI, and PLOS ONE, were searched. The search involved the use of the following combinations of keywords: “IoT smart home”, “home automation”, “cybersecurity”, “privacy”, “intrusion detection”, “lightweight cryptography”, “blockchain”, “edge computing”.

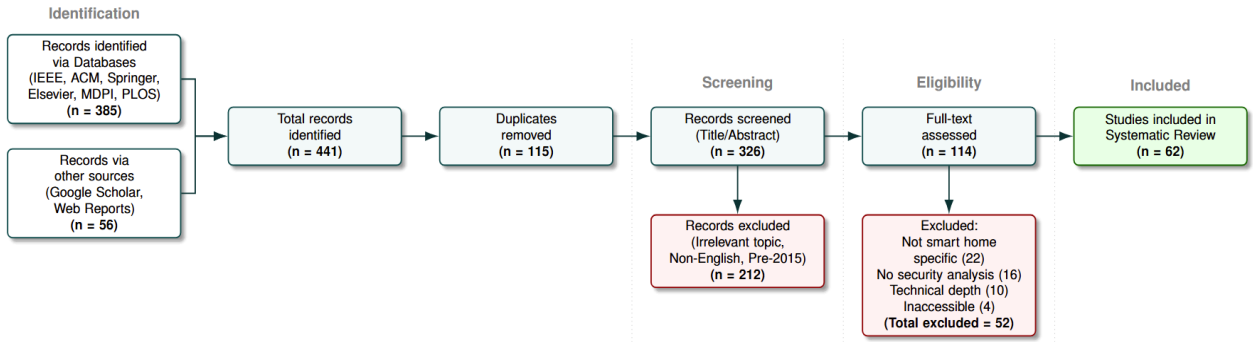


Fig. 1. PRISMA flow diagram detailing the selection process of the 62 studies included in this review.

The first search resulted in 441 records as shown in Fig. 1. Following elimination of duplicates and screening of titles and abstracts, 326 articles were left out. Articles were included in the review when they—

- Dealt with IoT-based smart home systems.
- Included some technical or analytical information about the system architecture, security vulnerabilities, or mitigation mechanisms.
- Were published in full text and in the English language.

The exclusion criteria applied in this study are-

- Non-peer-reviewed.
- Duplicate publications or multiple papers reporting the same study without additional insights.
- The articles with limited technical coverage, those that only covered non-residential IoT settings.
- The ones which were not directly pertinent to the research questions identified in the present study.

The last data set consisted of 62 studies.

3. Background, Motivation and Overview

The IoT is a new way to connect things, physical objects or environments via the internet, allowing them to communicate with each other without human intervention. In the smart home field, IoT enhances capabilities through embedding ordinary objects into intelligent networks [12]. These systems enable the automatic control of lighting, air conditioning and security to create controlled and dynamic environments. Examples include adapting heating and cooling to external weather conditions on IoT-connected devices, real-time intrusion detection and energy efficiency modelling. As a result, IoT improves user comfort, safety and energy efficiency, while facilitating lower operational costs [13–15].

At the core of these smart-home setups are microcontrollers that provide the system's intelligence. Examples include the ATMEGA2560, which is a powerful microcontroller widely used in custom automation projects due to its ability to manage multiple inputs and outputs efficiently [16]. In addition to that, there is the ESP8266, a compact Wi-Fi module that enables basic wireless functionality in IoT applications [17], and the Raspberry Pi, a versatile single-board computer capable of handling higher-level tasks such as data processing and complex software control [18]. Smart home environments empowered by IoT are also enriched with a variety of sensors which can capture several aspects of the domestic environment. These range from basic temperature and humidity sensors for hot/cold climates to advanced gas and fire sensors that can detect leaks and harmful environments. Furthermore, environmental sensing devices such as air quality and light-level sensors not only cover the immediate safety concerns but also contribute to overall occupant welfare. Together, these sensing mechanisms provide a clear infrastructural base for the development of proactive applications. Applications can be found in trigger generation of alerts/Virtual PEVAC smoke detecting systems and smart energy management that optimizes resource usage with respect to room occupancy [13–15, 19].

3.1. Technological Evolution and Architecture

Smart home systems of today have entirely transformed over the years from basic automation devices such as simple programmable timers for turning lights on and off at set times or remote controls used for operating some traditional appliances into multi-layered, sophisticated architectures involving advanced technologies which make our living environment more dynamic and responsive as shown in Fig. 2.

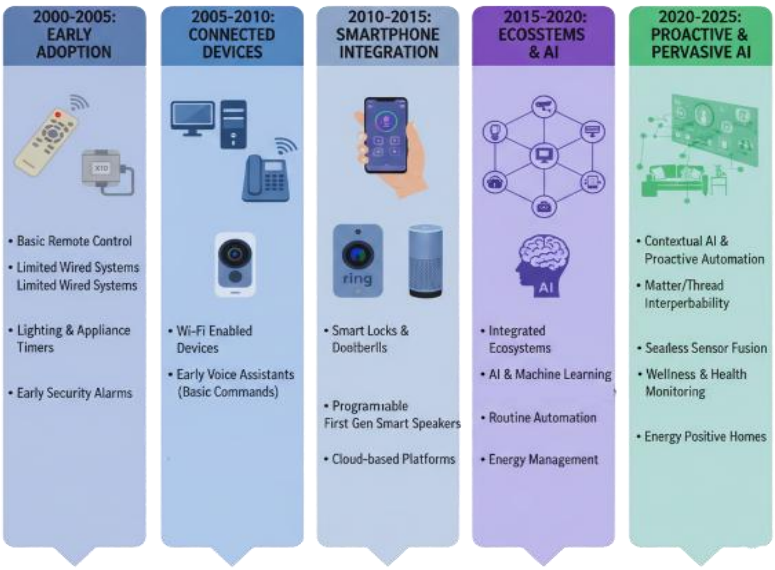


Fig. 2. Evolution of technology deployed in smart homes over time.

This evolution points to the growing maturity of smart home technologies and a drive toward integrated solutions, demanding that homes become intelligent living environments that know when you want things to happen, how devices should be connected together and have mechanisms in place to help better protect your family. The structure of such systems is conventionally described as a three-tier architecture. The perception layer includes the sensory devices for real-time environment sensing. The second (network) layer is responsible for directing data transmission across devices. Last, the application layer is responsible for interpreting the collected data, taking care of the user-friendly interface, and providing automation to a number of daily tasks. In this layered structure, not just advanced automation is feasible, but also artificial intelligence can be integrated, so that smart homes are actually becoming more adaptive and energy-aware (and user-centric) eventually serving as a personalized digital assistant [20–22]. Physical devices and sensors at the perception layer are used to monitor changes in the environment, while data can be transmitted through a variety of communication protocols (Wi-Fi, Bluetooth, Zigbee, Z-Wave, MQTT) by means of the network layer [14, 15, 22]. At

higher layers of the stack, the system becomes more intelligent by leveraging historical data and AI/ML algorithms. Advanced implementations have demonstrated scheduled appliance control, voice and facial recognition, as well as deep learning–based CNNs for enhanced automation and user personalization.

3.2. User Interface and Interaction Paradigms

The smart home interface space has become multi-modal as systems might use four major interaction modes including graphic interface through apps and web dashboards, voice agents such as Amazon Alexa or Google Home, physical interfaces such as programmable switches, and sensor-driven systems using gesture or motion recognition [24]. Graphical interfaces frequently dominate and even though we have arrived in the voice interaction era, the older population will be reticent to such modes of interaction as currently offered; not to mention universal design or a safety net for varied groups of users [13, 24].

3.3. Adoption Drivers and Barriers

In general, performance expectancy is still by far the strongest driving force behind user acceptance of IoT applications in residential settings since it shows a somewhat objective view of all potential benefits and value which users expect from using this technology. In addition, one of the most important requirements is widespread trust in the security, privacy and reliability features of IoT systems. Hedonic motivation, the entertainment effect or enjoyment received from using smart devices, has also proven to be a significant driver of adoption and meanwhile effort expectancy (the perception that using the technology is free of effort) will reduce barriers. Influence from peer usage and recommendations, or societal trends also have an impact on the kinds of users who adopt IoT solutions in their homes [25]. In Fig. 3, a comparative synthesis of often reported adoption drivers of IoT-based smart home systems is gathered based on previous empirical and survey-based research. The most common themes in literature point to energy efficiency gains, residential security, and convenience to users as the main reasons why the technology should be adopted [26–28]. The values of the relative importance in the figure are determined by the frequency and the emphasis of the mentioned drivers in the reviewed literature as opposed to original surveys or statistical measures on the population levels. In previous research, Fig. 4 is a summary of barriers that have been frequently cited to prevent the adoption of IoT smart homes. High start-up expenses, inability to interoperate with heterogeneous devices and issues with data privacy/security are recurrently cited as significant obstacles to adoption [29–31]. Just like in Fig. 3, the scores depicted are qualitative and literature-based, comparing the reported trends, but not direct survey results. Collectively, these numbers give a general idea of the most influential adoption motives and obstacles as represented in the current peer-reviewed literature.

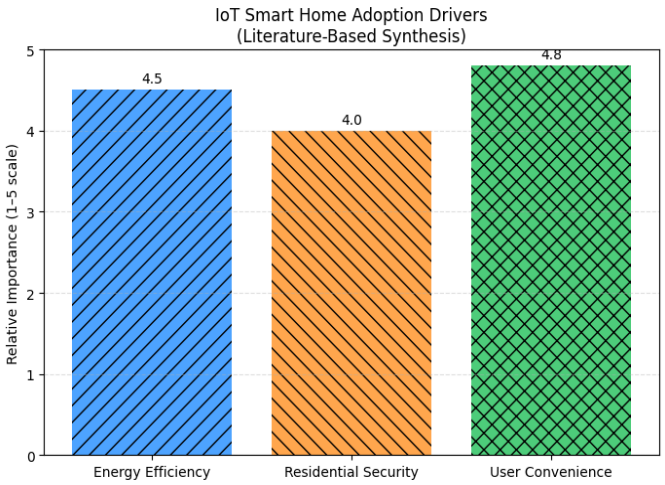


Fig. 3. Literature-based synthesis of commonly reported adoption drivers of IoT-based smart home systems where values are normalized on a 1–5 scale for visualization purposes and do not represent results from a single survey or population-level quantitative measurements.

3.4. Security Landscape and Threat Taxonomy

IoT based smart home automation is common and as a result we are now dealing with a layered landscape of threats that target the different layers: physical, network and application. We will all have more connected devices in our lives and homes, which expands the attack surface and introduce vulnerabilities that attackers can exploit. Physical vulnerabilities are unauthorized access to a device and tampering with software. Network level threats include data interception, denial of service and unauthorized access. Moreover, in addition to these piece-level vulnerabilities, there are a lot of software security issues at the application layer: for example, insecure APIs and a lack of protection such as authentication. The evolving risk environment requires strong, multi-layered defense, which drives the demand for safe and smart home security systems [20–22,32,33]. Fig. 5 presents the distribution of IoT smart home security

vulnerability categories based on a frequency-based synthesis of prior literature. Network-layer threats account for 38% of the vulnerabilities reported across reviewed studies, followed by device-centric vulnerabilities (29%), cloud-based risks (22%), and AI-targeted attacks (11%). These proportions reflect the relative prevalence of vulnerability categories identified through systematic analysis of 62 peer-reviewed studies, rather than survey-based or real-world attack incidence data [33]. It is clear from these figures how challenging aspects of security may be at various levels of the IoT architecture and how large the attack surface can be. The literature identifies common attack vectors, including unauthorized access, eavesdropping on data and conversations, malware injection, device takeover, denial-of-service (DoS), and advanced social engineering–based spoofing techniques [20–22, 32]. Furthermore, the huge heterogeneity of IoT devices and their constrained computational resources, limited energy, as well as the absence of any common security protocols or mechanisms across different vendors and platforms make it more difficult for applying end-to-end security [20, 33]. Although IoT security best practices tend to focus on defense in depth, and these multiple layers of security, this end-to-end challenge is also expected to require inter-device integration as well as adherence to the same standard security frameworks.

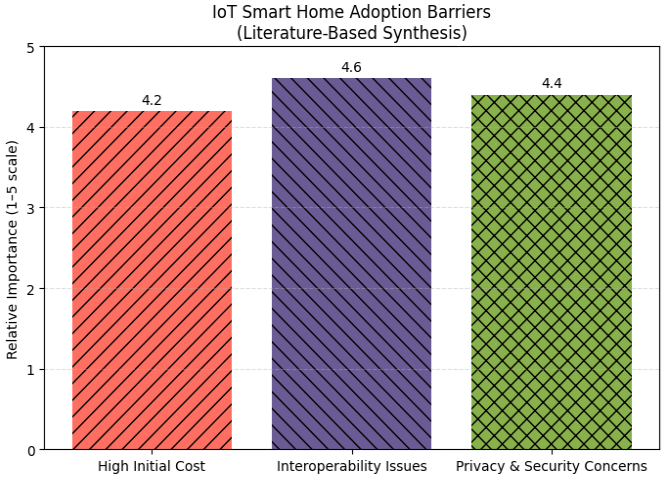


Fig. 4. Relative importance of frequently cited barriers to IoT smart home adoption synthesized from prior studies. The scores are derived from qualitative aggregation of existing literature and do not correspond to direct survey percentages or time-specific datasets.

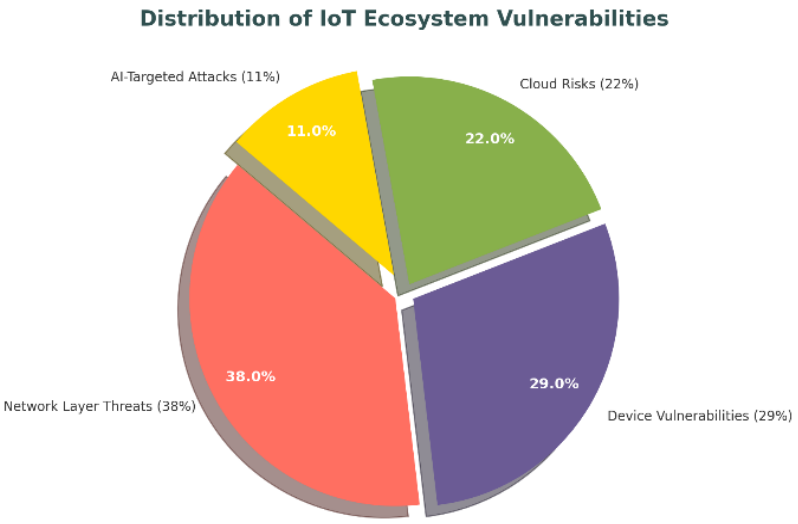


Fig. 5. Distribution of IoT smart home security vulnerability categories derived from frequency-based classification reported in systematic literature reviews, illustrating relative prevalence across network-layer, device-centric, cloud-based, and AI-targeted threats [33].

3.5. Privacy Concerns and User Awareness Gap

Empirical analysis conducted across more than 40 household studies reveals a notable discrepancy between expressed user concerns and actual behavioral practices regarding privacy and security in IoT environments [34]. Although participants frequently emphasized apprehensions related to unauthorized tracking, privacy violations, data breaches, and potential misuse of personal information by manufacturers or government entities, their adoption of effective safeguards remained limited. This gap can be attributed to multiple factors, including the inherent complexity

of technical security mechanisms, poorly designed user interfaces from a security perspective, and a general lack of comprehension regarding effective protection models [34]. These findings highlight the critical need for IoT systems to incorporate robust default privacy configurations, transparent data management frameworks, and user-friendly security control interfaces. Such measures can reduce reliance on expert users, accelerate the adoption of protective behaviors, and mitigate the well-documented disparity between user concerns and actual security practices [22, 34].

3.6. Countermeasures and Emerging Solutions

There are several IoT vulnerabilities countermeasures that have been suggested by the research community such as AI-driven anomaly detection, post-quantum cryptography algorithms, and blockchain-based authentication systems, among others [20–22, 32, 33]. These methods have been demonstrated to improve attack detection and mitigation but there is a range of reported effectiveness in the literature. The zero-trust security model provides more intrusion prevention instances yet may demand a full overhaul of the infrastructure in general [33]. Foundational security improvements are offered by hardware-based protection, including Physically Unclonifiable Functions (PUFs), secure booting, and tamper-resistant chipsets [21, 22].

3.7. Open-Source and Privacy-Preserving Approaches

To protect user privacy in scenarios dependent on cloud services, open-source frameworks like qToggle offer local control over smart home operations [15]. These solutions offer a balance between functionality, cost, and user privacy, while promoting community-driven development and customization [15]. Similarly, edge computing enables local data processing, thereby enhancing privacy by minimizing data transmission to external servers [20, 22].

3.8. Research Motivation and Scope

As smart home technologies evolve at a rapid pace, so do the associated privacy and security challenges. While early developments focused on functionality and user experience, modern systems must incorporate security and privacy as core components, especially when scaled for mass deployment [13–15,19–22,24,25,32–34]. This review aims to provide a holistic understanding of the IoT-based smart home ecosystem by evaluating the technological foundations, identifying key security threats, and assessing available countermeasures to inform future research and implementation practices. A consolidated overview of the primary features, challenges, and research directions derived from this review is presented in Table 1. Given the increasing adoption rates, the growing sophistication of attack vectors, and the evolving regulatory environment, integrated approaches that combine technical safeguards, user-centered design, and policy frameworks are essential [22, 25, 33, 34]. Such integration will bridge current knowledge gaps and provide actionable insights for researchers, developers, and policymakers working to ensure secure and privacy-respecting smart home technologies.

Table 1. Summary of Key Research Motivations, Challenges, and Future Directions in IoT-Based Smart Home Systems.

References	Key Aspect	Insights from Review	Implication for Future Work
[1, 2, 25, 35]	Adoption Trends	Rising adoption driven by convenience, energy efficiency, and perceived security benefits; however, trust, interoperability, and upfront cost remain decisive for uptake.	Quantify drivers/barriers with user studies; align design with privacy-by-default and clear data handling.
[3–6, 20, 21, 32, 33, 36, 37]	Security Challenges	Sophisticated attack vectors span device, network/protocol (Wi-Fi, Zigbee, Matter), cloud/app, and AI layers; real deployments expose weak auth and insecure APIs.	Prioritize layered threat modeling; evaluate protocol- and app-level weaknesses in integrated environments.
[1, 3, 6, 22, 35, 37, 38]	Privacy Concerns	Users express strong privacy concerns yet often lack effective safeguards or usable controls; surveillance/profiling and misconfigurations are common.	Develop intuitive privacy controls and safe defaults; deliver onboarding and continuous nudging to reduce misconfigurations.
[1, 7–11, 19, 20, 34, 36, 39, 41]	Countermeasures	Lightweight cryptography, ML/DRL-based IDS, blockchain-based authentication, and PQC show promise but can be compute/energy heavy.	Co-design for constrained hardware; benchmark accuracy vs. overhead; support incremental deployment in real homes.
[3, 4, 13–15, 36, 40–43, 46]	Interoperability & Protocols	Heterogeneous stacks (Zigbee, Z-Wave, Wi-Fi, Matter) create integration gaps and new attack surfaces; controlled trust and protocol updates are critical.	Standardize protocol security baselines; certify cross-ecosystem interoperability; continuously verify controllers/bridges.
[1, 34, 47]	Edge/Federated Analytics	Edge/fog and federated approaches enhance privacy and enable collaborative IDS, reducing cloud exposure	Develop FL/edge IDS tailored to smart-home constraints; ensure robustness against poisoning and aggregation attacks.
[1, 5, 8, 37, 47, 48]	Evidence & Datasets	Public datasets and shared traces (e.g., IDS evaluations; forensic models; appliance/load datasets) enable reproducible evaluation.	Adopt shared benchmarks; publish datasets; report compute/energy footprints alongside detection metrics.
[1, 6, 9, 11, 22, 35, 38, 41]	Integrated Approach Needs	Technical safeguards alone are insufficient; coupling with usability, governance, and compliance is essential for trust and sustained adoption.	Build holistic frameworks integrating technical, human-centered, and policy-oriented measures.

4. IoT Technologies in Smart Homes

IoT technologies serve as the ground infrastructure for intelligent home systems, acting as an enabling platform for multifarious household areas, offering connectivity, automation, and intelligent decision-making. Sensors, actuators, communication protocols, and processing units are key components in the formation of an intelligent environment that provides energy savings, security, and convenience to the user [13–15, 39]. Fig. 6 illustrates the overall IoT-enabled smart home architecture, depicting the integration of sensors, actuators, processing unit, gateway, cloud server, and remote user access, along with the communication flows between them. To complement this architecture, Table 2 summarizes the major IoT technology areas, their key functions, and representative references discussed in this section.

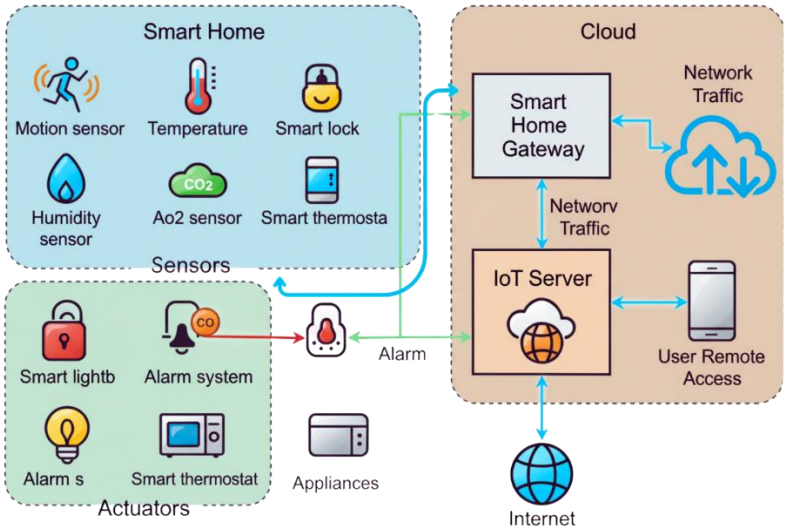


Fig. 6. IoT Smart Home System illustrating sensors, actuators, gateway, IoT server, remote access, and alarm communication flows.

Table 2. Summary of IoT Technologies in Smart Homes.

References	Technology Area	Key Features / Functions	Representative Examples
[13–15, 19, 20, 26, 42]	Sensors and Actuators	Capture real-time data (temperature, humidity, motion, light, gas, fire, vibration); enable automatic responses such as lighting control, alarms, HVAC adjustment.	PIR sensors, flame detectors, gas sensors, multimodal sensors for elderly care/energy monitoring.
[14, 15, 20, 22, 32, 33, 40]	Communication Protocols and Networking	Provide device interconnection, low-latency transmission, scalability, and resilience; employ mesh or LPWAN topologies; integrate security features such as encryption and authentication.	Wi-Fi, Zigbee, Z-Wave, Bluetooth, MQTT, Thread, LoRaWAN.
[13–15, 19, 36, 39]	Controllers and Processor Units	Aggregate data, enforce automation rules, integrate with cloud/AI analytics; modular and open-source designs improve scalability and privacy.	ESP8266, NodeMCU, Raspberry Pi, ATMEGA2560, qToggle frameworks.
[19, 21, 25, 40, 44]	Advanced Features: AI and Blockchain Integration	AI enables predictive controls, anomaly detection, and optimization; blockchain ensures decentralized authentication and tamper-proof data integrity.	CNN-based appliance status classification, blockchain-based authentication frameworks.

4.1. Core Components: Sensors and Actuators

At the heart of smart home IoT ecosystems there lies a set of sensors gathering real-time environmental data about temperature, humidity, motion, gas leaks, fire hazards, light intensity, and vibration. These sensors communicate with actuators to allow automatic responses, such as dimming lights or setting off alarms [13–15, 19]. Passive infrared (PIR) sensors, for example, detect human presence to trigger security protocols, whereas flame and gas detectors reduce any dangers by sending out immediate alarms [14, 20].

The selection of sensing modalities is driven not only by functionality but also by trade-offs involving energy consumption, privacy preservation, deployment cost, and system scalability. PIR sensors are widely preferred over camera-based sensing due to their low power requirements and privacy-friendly operation, which is critical in residential environments [53].

Some of the sophisticated implementations employ multimodal sensors for thorough monitoring to facilitate programs in elderly care and energy management [13, 42].

Multimodal sensor fusion improves robustness and contextual awareness by compensating for the limitations of individual sensors, particularly in complex scenarios such as activity recognition and safety monitoring [54].

4.2. Communication Protocols and Networking

Reliable communication is critical for IoT-enabled smart homes, with protocols like Wi-Fi, Bluetooth, Zigbee, Z-Wave, and MQTT facilitating data exchange between devices and central hubs. These protocols ensure low-latency, secure transmission over perception, network, and application layers, often employing mesh topologies for extended coverage and resilience [14, 15, 20, 22].

High-bandwidth protocols such as Wi-Fi offer ease of integration but incur higher energy consumption, whereas low-power protocols like Zigbee and Z-Wave are better suited for battery-operated devices and dense sensor deployments [28].

Emerging standards, such as LoRaWAN and Thread, enhance scalability in resource-constrained environments, reducing power consumption while maintaining interoperability [20, 22].

However, reduced data rates in low-power wide-area networks limit their applicability for latency-sensitive smart home services [55].

Security features, including encryption and authentication, are integral to these protocols to protect against vulnerabilities like eavesdropping and denial-of-service attacks [13, 32, 33, 36].

Protocol selection therefore represents a balance between performance, energy efficiency, interoperability, and security assurance [56].

4.3. Controllers and Processor Units

Microcontrollers such as ATMEGA2560, ESP8266, NodeMCU, or even a Raspberry Pi form the processing backbone, wherein they take charge of data aggregation, rule-based automation, and linking with cloud platforms, all supported by AI-driven analytics, such as CNNs for predictive appliance controls with accuracies above 96% in status classification [13–15, 19].

Low-cost microcontrollers are favored for large-scale deployment, but their limited computational capacity constrains the execution of advanced analytics at the device level [57].

Modular designs are a focal idea behind open-source frameworks such as qToggle—locally processed to provide a veil of privacy and reduce dependence on the cloud [13, 39, 40].

Edge-based processing reduces latency and enhances data privacy by minimizing continuous data transmission to cloud servers, supporting a hybrid edge-cloud architecture for smart homes [19,39,40,58].

4.4. Advanced Features: AI and Blockchain Integration

Integrating modern AI means detecting anomalies and optimizing energy systems, along with using blockchain for decentralized authentication and data integrity. These features address upscaling issues and allow predictive maintenance and adaptive automation [19, 21].

AI-driven models enable context-aware decision-making by learning user behavior patterns, thereby improving system efficiency and responsiveness over static rule-based approaches [40, 47].

Sufficient empirical evidence exists in support of 20–25% energy savings and improved interoperability, but economic constraints, a lack of standard approaches, and device heterogeneity remain primary barriers [25, 40, 44].

While blockchain enhances trust and tamper resistance in multi-vendor ecosystems, it introduces additional computational overhead and latency, limiting its applicability for real-time control operations [7,19,59].

Such integration of IoT fosters resilient, user-centric smart homes and has motivated further research in the areas of privacy-preserving designs and standardization efforts [20, 22, 33].

5. Security Risks and Threat Landscape

The fast increase of IoT-enabled smart homes has created an increasingly complex security landscape ranging across hardware, software, network, and user domain vulnerabilities. Fig. 7 shows the scenario of different types of attacks that can occur in smart home systems. The multifaceted threat environment, therefore, gives rise to the understanding of both the intrinsic limitations of the devices and the added improvisations malicious actors have been employing to exploit them.

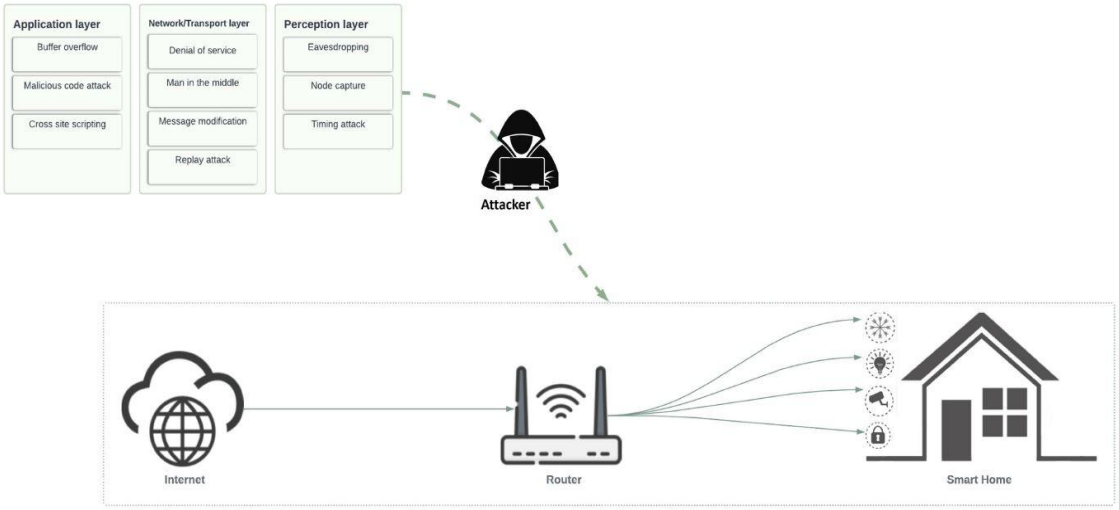


Fig. 7. Security attacks in smart homes [20].

5.1. Device-Level Vulnerabilities

The computation capability of popular smart home devices is often rather low and the integrated security mechanisms are usually weak, especially in authentication, access control, data encryption etc. Usually, such restrictions follow from cost considerations and trade-offs in use [32, 33]. A large number of such devices are provisioned with default or vulnerable credentials, which makes them more vulnerable to brute-force and credential stuffing attacks [24]. Besides that, device firmware/operating systems are commonly not regularly patched by device vendors for security updates and are vulnerable to attacks using known vulnerabilities [33]. This is primarily a hardware-level issue, but failures can also occur due to physical tampering or supply chain attacks. Such incidents may lead to data leakage, installation of rootkits, or even complete alteration of device functionality. These security and privacy threats are not just theoretical and have been demonstrated in popular consumer smart home products. For example, IP cameras from companies such as D-Link and TP-Link are known to come with default passwords as well as outdated firmware and are frankly easy targets for brute forcing or unauthorized remote access [60].

5.2. Network and Protocol Threats

Weaknesses in network configuration are a principal point of entry for intruders. Unsecured communication channels, unencrypted data transmission, and thirdly: providing too many or open network services so that sensitive information can be exposed on the way and into the home network [20, 22, 33]. Typical attack types are man-in-the-middle, denial-of-service (DoS), traffic eavesdropping, or device fingerprinting, to disrupt the service or to steal data. Without segmentation, a single device compromise could pose risks to the entire home ecosystem [20].

5.3. Malware, Botnets, and Automated Exploitation

IoT botnets such as Mirai are enlisting smart home devices to join their ranks, either in DDoS campaigns or to serve as conduits for the proliferation of malware within residential networks. Once in, they can deploy ransomware to demand a fee from targets in exchange for regained access or use rootkits that can sit undetected on systems for months. Recent news reports show that botnet and malware attacks are increasingly frequent in home IoT devices.

5.4. Data Privacy and Surveillance

The data from smart home sensors provides a rich set of targets for privacy invasions and identity theft, ranging from daily routines and behavioral patterns to audio/visual recordings [22, 29]. If the devices are vulnerable, they can lead to unauthorized entities sharing personal data through leaks in the cloud or via weak APIs, sometimes allowing attackers to eavesdrop or interfere with occupants' behavior from a distance [22, 35]. Previous research has shown that smart cameras and baby monitoring systems can expose audio-visual data when encryption is weak, authentication and access control are insufficient, or the systems operate in poorly configured or adversarial network environments [61].

5.5. Interconnectedness and Compounded Risks

By their very nature, interconnected smart homes magnify risk: should a single device be compromised, the mechanism can be used as a point of pivot against other systems—unlocking doors and windows, attacking intruder alarms, or even selecting and operating smart appliances [21]. The lack of standardized security policies and inconsistent enforcement of even basic protections remains a major source of vulnerability.

5.6. Human Factors and Security Awareness

Many users simply do not change default passwords, install firmware updates, or configure basic security settings of their device [34]. As the research shows, the gap between the perceived risk and the effective mitigation at an average home level remains huge, thus contributing to the exposure being higher than it should be [34, 37]. Overall, the security of smart home systems is limited by technical constraints as well as the lack of an established security definition and human factors. With the changing threat environment, optimal countermeasures should have a multi-layered nature. These strategies should include device hardening, use of encrypted communication protocols, and strong authentication methods as well as frequent policy and firmware updates while employing network segmentation. User training is also essential and the regular creation of security awareness by industry and academic research communities will help to maintain adaptive, resilient protection in practical deployments. These instances demonstrate that security vulnerabilities in smart home systems frequently arise not from a single point of failure, but from a combination of constrained device resources, inconsistent firmware update mechanisms, network misconfigurations, and user behavior. Consequently, the threat landscape discussed in this paper reflects realistic deployment scenarios commonly observed in contemporary consumer IoT ecosystems.

6. Countermeasures and Security Mechanisms

Several studies have suggested many security mechanisms to prevent the diverse attack strategies on IoT-enabled smart homes at different levels of system architecture.

Lightweight cryptographic algorithms have been of interest in the context of this paper as a means to provide secure communication between devices without imposing too much computation on resource-constrained nodes [49] and are considered fundamental. At the same time, blockchain-based structures seem to be most powerful constructs for decentralized storage platforms in a way that prevents unauthorized data alteration or access also the design of anti-corrupted mechanisms [50].

Recent security frameworks incorporate an increasingly formalized type of risk analysis [38]. Such techniques can be effective to determine whether firmware is genuine, make use of biometric authentication devices, and secure the data being transmitted by encrypted means while also augmenting cyber-security as well as physical security.

AI-based intrusion detection systems (IDSs) also have a superior capability to detect new types of attacks than traditional rule-based approaches [15,41]. Unlike static rule sets, machine learning-powered detection learns from past attack patterns and starts responding dynamically to emerging threat vectors. Other applications to improve physical security and more precisely discriminate unauthorized presence or motion are multi-sensor intrusion detection systems with classification algorithms [51].

At the level of communication protocols such as Zigbee [36] and MQTT, new standards have almost all added high-level encryption standards (AES) that not only have increased defenses against common cyberattacks like eavesdropping or man-in-the-middle exploits but have also given rise to new types of attacks [48]. Conflict detection frameworks have also been proposed as a method for detecting and correcting inconsistencies in automation rules through which both the operational safety and security of the system are improved [52].

Local data processing is another way to better secure the IoT smart home: edge computing is particularly suitable for real-time and security-sensitive applications as edge reduces latency, and provides significant advantages for data privacy [34, 47].

7. Comparative Analysis

Security measures designed for smart homes differ largely in effectiveness, scalability and practicality. In this paper, through a comparative analysis we provide insights into the strengths/weaknesses of various approaches from technical and user-centric views.

Intrusion detection systems (IDS) based on artificial intelligence (AI) have achieved promising results to detect complex and adaptive threat patterns [15,41]. Because of their adaptive capability, they could potentially react to new attack vectors on the fly and help in securing IoT environments in an ever-evolving threat landscape. Nevertheless, these benefits often go hand in hand with the reduced computational capabilities inherent to embedded IoT systems [13, 47], as these devices often do not have the processing power and memory to support continuous learning processes or store large datasets necessary for effective operation of AI models, limiting the scalability in resource-constrained contexts.

In terms of communication protocol, both Zigbee and MQTT support mechanisms to ensure secure data transmission by using encryption [36, 38]. Yet, the largest adoption still belongs to Wi-Fi being the global standard supporting high speeds and numerous other connectivity goals important for smart homes. More importantly, the prevalence of Wi-Fi also leads to a widened attack surface and an attractive target for intruders to impact or penetrate it from unauthorized source [37], hence Wi-Fi becomes one of the most popular areas receiving attention in security enhancements.

Using blockchain technologies, data storage and verification can be made decentralized while still being tamper resistant for the sake of data integrity and traceability [50]. At the same time, while their distributed consensus mechanisms deliver a strong resistance to manipulation, the computational and energy resources they require are too high for low-power IoT sensors, nodes and networks. Another approach is Bayesian monitoring frameworks which provide a probabilistic model that balances analytical capability and resource consumption to allow real-time security monitoring without putting much pressure on the system resources [41].

User behavior has a huge impact on security outcomes from the human-factor perspective. Misconfiguration, negligence, and user unawareness are documented in the literature to be the main vulnerabilities that affect smart home environments [24,33,35,37]. Solutions include user-centered security designs that focus on simplicity in configuration interfaces and enforce secure behaviors by default to reduce exposure to user-induced vulnerabilities [47]. In the end, field deployment experience has revealed inherent interoperability problems in environments with various vendor devices [45], which continue to persist. Such inconsistencies can ultimately lead to security gaps that go unnoticed, reinforcing the requirement for a standard communication protocol and certification framework to enable consistent enforcement of security across devices.

8. Future Direction

Present activities and potential solutions to some of the security problems envisaged in smart home scenarios are presented along with early results. Several emerging research trends indicate the direction of future developments in smart home security.

The production of energy-efficient AI models that are executable on edge resources is one of the most promoted topics. Federated learning and model pruning are two of them, showing that these technologies are capable of providing on-device, near real-time inference without relying on cloud infrastructure while also reducing data latencies and maintaining the privacy of user data. In parallel, zero trust security models have gained popularity. The foundation of these frameworks is that, by default, every device is untrusted and therefore should be continuously authenticated and verified, while various dynamic probabilistic models are used to detect abnormalities [41].

Interoperability remains a big problem, particularly in heterogeneous environments with many different vendors involved. It can be demonstrated from the analysis of the results of other studies [17, 19, 20] that standard communication protocols and open APIs are needed to avoid any complicated integration of devices. Not only can functional portfolios work together, but fragmented or proprietary architectures that may pose risks are also eliminated.

Since design focuses on users, there is more of an emphasis on usability and the necessity to find a solution that balances security. We then demonstrate that using interactive tutorials, real-time alerts and secure-by-default configurations in smart home platforms can reduce the occurrence of user-induced vulnerabilities, as shown by available empirical evidence [24, 35, 37]. Deploying such measures is what turns a user from making ‘informed security decisions’ into making ‘well-informed’ ones, not counting on whether (and how much) did the human user pay “attention” to themselves.

Cross-disciplinary innovation also spans more than one field. For example, deep learning–based classification models such as convolutional and autoencoder architectures, which have demonstrated strong performance in pattern recognition tasks, have been successfully adapted for context-aware anomaly detection in IoT and smart home environments, enabling more accurate identification of abnormal network behavior and security threats [15].

Post-quantum cryptography is another strategic research frontier. The technological progress of quantum computing also requires the design of lightweight quantum-resistant encryption schemes to protect communications in smart home networks that are expected to function on constrained-capacity low-power devices [50].

Each innovation on its own represents a step forward, but together they are the building blocks for next generation smart home security architectures: intelligent systems, interoperable solutions, and user-friendly yet resilient designs Adaptation, sustainability, and long-term security of connected home environments all necessitate the integration of these approaches as we continue to evolve the IoT landscape [38, 49].

9. Response to the Research Questions

This section revisits the research questions articulated in the Introduction and synthesizes the insights derived from the reviewed literature. By explicitly addressing each question, it situates the technological, security, and human-centric dimensions of IoT-based smart homes within a coherent framework and highlights where progress has been achieved and where challenges remain unresolved.

RQ1. What are the key technological enablers of IoT-based smart homes, and how do they interact to support automation, security, and user experience?

The foundations of smart homes lie in sensors, actuators, controllers, and communication protocols, which collectively enable data collection, automated decision-making, and connectivity [13]. System architectures built on these components deliver efficiency and convenience but also increase system complexity [14]. Advanced enablers such

as AI-driven analytics are increasingly integrated to optimize energy use and enhance user experience [15]. Similarly, blockchain-based trust models have been proposed to secure device-to-device communication [7], while edge and federated computing architectures reduce latency and preserve privacy by shifting computation closer to the data source [47]. Recent work also explores quantum-resilient architectures that combine blockchain and decentralized storage for long-term protection of smart-home systems [10]. Collectively, these technologies illustrate how functional benefits are tightly coupled with new security requirements.

RQ2. Which security vulnerabilities most significantly impact smart home environments across device, network, cloud, and application layers?

Vulnerabilities extend across all layers of the smart-home ecosystem. At the device level, weak authentication and outdated firmware expose endpoints to attacks [32]. At the network level, protocol weaknesses in Zigbee, Z-Wave, and Thread have been empirically demonstrated, highlighting flaws in confidentiality and access control [4]. Even encrypted traffic can be exploited for profiling, demonstrating systemic privacy risks [3]. At the application and cloud levels, insecure APIs and automation-rule inconsistencies remain recurrent problems [52]. Intrusion detection experiments show that IDS tools differ widely in performance when applied to smart-home traffic, with limitations in scalability and configuration robustness [5]. Furthermore, forensic analyses emphasize that accountability and evidence preservation mechanisms are often missing from deployed systems [6]. These findings indicate that vulnerabilities are not isolated, but interconnected across system layers.

RQ3. How effective are the countermeasures and frameworks in addressing the unique constraints of resource constrained smart home systems?

A wide spectrum of countermeasures has been introduced. Lightweight cryptographic algorithms ensure confidentiality and authentication with minimal computational overhead, making them suitable for resource-constrained IoT devices [49]. Surveys highlight their importance for scalability in large-scale deployments [2]. Blockchain frameworks support tamper-proof authentication and distributed trust management, improving resilience to centralized failures [6]. Forensic-ready blockchain-based process models have also been proposed to improve transparency in investigations [8]. AI-based intrusion detection systems adapt to evolving threats and achieve higher detection accuracy than rule-based methods [15], while experimental evaluations confirm their potential but caution about resource overheads [5]. Finally, research into post-quantum cryptography and quantum-assisted blockchain anticipates the need to protect smart homes against quantum-capable adversaries [11]. While each countermeasure shows promise, hybrid layered defense strategies are increasingly recognized as the most practical path for deployment.

RQ4. Where do gaps remain, and what future directions are most critical for advancing secure smart home deployments?

Three gaps are particularly evident. First, interoperability remains an enduring challenge, as heterogeneous devices and protocols continue to fragment the ecosystem and prevent unified enforcement of security baselines [45]. Second, user centric security designs are underdeveloped; surveys repeatedly show that users lack intuitive privacy controls and default secure configurations, eroding trust [1]. Third, the emergence of quantum-era threats underscores the urgency of developing post-quantum cryptography schemes and integrating them into IoT ecosystems [9]. Forensic and accountability frameworks must also mature to ensure that breaches can be reliably investigated and attributed [6]. Addressing these gaps requires collaborative efforts across academia, industry, and regulatory bodies to align technical innovation with usability and compliance.

10. Discussion

The responses to all of the research questions highlight how a multi-tiered technological framework made up of sensors, controllers, communication protocols, and AI-driven analytics supports IoT-based smart homes. These components expand the attack surface across the device, network, cloud, and application layers even though they offer efficiency, automation, and personalization. Although current countermeasures, such as edge computing, blockchain-based authentication, intrusion detection systems, and lightweight cryptography, show great promise, they are hampered by a lack of cross-vendor compatibility, device heterogeneity, and limited processing power. Therefore, it appears that the most practical way to achieve strong smart home security is to implement a hybrid defense approach that incorporates many tactics.

The analysis emphasizes how crucial it is to incorporate privacy and security into the design of smart homes. This involves investing in energy-efficient AI models designed for limited contexts, ensuring device compliance, and implementing interoperable standards for industry stakeholders. Enforcing privacy-by-default regulations and providing incentives for the implementation of security frameworks are two important roles that policymakers and regulators can play. In order to close the well-established gap between security worries and real protective measures, end users need secure-by-default configurations and intuitive interfaces.

This review is constrained by its dependence on secondary sources and the breadth of available literature. Although it encompasses trends until 2025, forthcoming empirical research may reveal new vulnerabilities or mitigation

measures not currently included. The lack of extensive deployment data limits the capacity to generalize results across various smart home settings. The review ultimately lacks a quantitative meta-analysis, which could enhance the validation of the comparative effectiveness of various countermeasures.

The results indicate multiple essential directions for subsequent investigation. First, the creation of quantum-resistant cryptography protocols suitable for restricted devices will be crucial in the next decade. Secondly, zero-trust security frameworks must be tailored to the resource constraints of smart home systems, guaranteeing ongoing verification without undue burden. Third, prioritization of human-centered security designs is essential, focusing on usability, awareness enhancement, and error-tolerant setups. Finally, cooperative initiatives among academics, business, and regulatory bodies are essential to create benchmark datasets, standardized testing methodologies, and interoperable security frameworks that guarantee uniformity across diverse IoT ecosystems.

11. Conclusion

Smart homes enabled by IoT have become an integral part of our day-to-day life by providing the latest automation features, comfort, and reduced energy usage. But, in the same vein, the interconnection and other efficiency which IoT has brought about by connecting so many new devices is also a double-edged sword, as it has also introduced vast amounts of security and privacy challenges increasing the attack surface. With smart technologies being increasingly accepted, it is becoming more important to secure and ensure the integrity and reliability of systems.

Our work in this paper is to provide insight into the security vulnerabilities in smart home ecosystems and propose some defensive solutions namely ultra-lightweight cryptographic protocols, AI-based threat detection systems, blockchain-enabled decentralized architectures, as well as privacy-preserving approaches. Some combination of these measures, deployed as part of an adaptive, layered-protection architecture, can provide long-lasting and strong protection against both cyber and physical threats.

However, the most advanced technical measures will still be vulnerable. Key human factors such as the mishandling or improper configuration of devices, poor security practices and a lack of education in cybersecurity still present serious dangers. As a result, secure-by-default, usability and in situ advice must be considered for future smart home design.

Over the next five years, smart home security will need to consider scalable and cross-vendor interoperable solutions against new threats, including preparation for post-quantum cryptography. Meeting this need will demand a combination of technological innovation, human-centered design, and policy-motivated regulation, to ensure the smart homes of tomorrow are not just smart and connected, but also secure by default.

All the Declarations and Statements

Author Contributions Statement

Tanvir Ahmed, Md. Akhterujjaman Siddiquee, Sheikh Sidratul Muntaha Punno – Conceptualization, Methodology, Data Curation: Proposed research ideas, Constructed the overall framework, Performed literature survey, data curation. They also drafted the initial manuscript and documented the technical background of the study.
Fahmida Ahmed Antara, Sadia Enam and Md. Moshiur Rahman – Review and Editing: Reviewed and edited the manuscript, ensured clarity and coherence, and helped coordinate research milestones and deadlines.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Statement Funding Declaration

This research received no external funding.

Data Availability Statement

Data sharing is not applicable to this article as no new data were generated or analyzed during the current study.

Ethical Declarations

This study did not involve human participants or animals, and therefore ethical approval was not required.

Acknowledgements

The authors express their gratitude to Nabonita Mitra, Ph.D. candidate at Texas Tech University, USA, for her invaluable help during the literature review process.

Declaration of Generative AI in Scholarly Writing

During the preparation of this manuscript, the authors used generative AI tools to improve language clarity, grammar, and readability. The authors carefully reviewed and edited the content, and take full responsibility for the accuracy and integrity of the work.

Abbreviations

The following abbreviations are used in this manuscript:

IoT – Internet of Things
AI – Artificial Intelligence
ML – Machine Learning
NLP – Natural Language Processing
CNN – Convolutional Neural Network
IDS – Intrusion Detection System
DoS – Denial of Service
DDoS – Distributed Denial of Service
MQTT – Message Queuing Telemetry Transport
Wi-Fi – Wireless Fidelity
LPWAN – Low Power Wide Area Network
API – Application Programming Interface
AES – Advanced Encryption Standard
PIR – Passive Infrared
PUF – Physically Unclonable Function
PQC – Post-Quantum Cryptography
PRISMA – Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RQ – Research Question
M2M – Machine-to-Machine
HCI – Human-Computer Interaction
CI/CD – Continuous Integration / Continuous Deployment

References

[1] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of smart-home security using the Internet of Things," Electronics, vol. 13, no. 16, p. 3343, 2024.

[2] K. Y. Najmi, M. A. AlZain, M. Masud, N. Z. Jhanjhi, J. Al-Amri, and M. Baz, "A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability," Materials Today: Proceedings, vol. 81, pp. 377–382, 2023.

[3] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A. R. Sadeghi, and S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!," in Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 207–218, 2020.

[4] F. Alsakran, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Intrusion detection systems for smart home IoT devices: experimental comparison study," in Int. Symp. on Security in Computing and Communication, pp. 87–98, Springer, 2019.

[5] S. F. Ahmed, S. S. Shawon, A. Bhuyian, S. Afrin, A. Mehjabin, S. A. Kuldeep, M. S. B. Alam, and A. H. Gandomi, "Forensics and security issues in the Internet of Things," Wireless Networks, pp. 1–36, 2025.

[6] H. Pourrahmani, A. Yavarinasab, A. M. H. Monazzah, et al., "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the blockchain," Internet of Things, vol. 23, p. 100888, 2023.

[7] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," Computers & Electrical Engineering, vol. 83, p. 106585, 2020.

[8] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in 2016 IEEE Symposium on Security and Privacy (SP), pp. 636–654, 2016.

[9] B. Yuan, F. Wu, and Z. Zheng, "Post quantum blockchain architecture for Internet of Things over NTRU lattice," PLOS ONE, vol. 18, no. 2, p. e0279429, 2023.

[10] G. Iovane, "A multi-layer quantum-resilient IoT security architecture integrating uncertainty reasoning, relativistic blockchain, and decentralised storage," Applied Sciences, vol. 15, no. 16, 2025.

[11] F. Ye, Z. Zhou, and Y. Li, "Quantum-assisted blockchain for IoT based on quantum signature," Quantum Information Processing, vol. 21, no. 9, p. 327, 2022.

[12] W. Sarada, K. V. Prashanth, A. B. Mary, K. Premkumar, V. P. Vijayan, et al., "IoT in smart homes: Enhancing lifestyle through intelligent automation and control," in 2025 Int. Conf. on Automation and Computation (AUTOCOM), pp. 336–341, IEEE, 2025.

[13] Y. Chen, H. Zhang, and S. Zhong, "Design and implementation of smart home system based on IoT," Results in Engineering, vol. 24, p. 103410, 2024.
[14] S. F. Islam, M. I. Hasan, M. Akter, and M. S. Uddin, "Implementation and analysis of an IoT-based home automation framework," Journal of Computer and Communications, vol. 9, no. 3, pp. 143–157, 2021.
[15] Y. Meidan, M. Bohadana, A. Mathov, S. Mirsky, D. Breitenbacher, A. Shabtai, and Y. Elovici, "N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," IEEE Communications Magazine, vol. 56, no. 9, pp. 172–179, 2018.
[16] M. G. Anduinta Rhizma and C. Suhendar, "Home security and fire detection system design using IoT-based microcontroller ATmega2560," GCISTEM Proceeding, vol. 1, pp. 1–9, 2022.
[17] S. A. Devi, M. Sitha Ram, K. Ranganarayana, D. Babu Rao, and V. Rachapudi, "Smart home system using voice command with integration of ESP8266," in 2022 Int. Conf. on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1535–1539, IEEE, 2022.
[18] W. A. Alonazi, H. Hamdi, N. A. Azim, and A. A. Abd El-Aziz, "SDN architecture for smart homes security with machine learning and deep learning," Int. J. of Advanced Computer Science and Applications, vol. 13, no. 10, 2022.
[19] M. Umer, S. Sadiq, R. M. Alhebshi, M. F. Sabir, S. Alsubai, A. A. Hejaili, M. M. Khayyat, A. E. Eshmawi, and A. Mohamed, "IoT based smart home automation using blockchain and deep learning models," PeerJ Computer Science, vol. 9, p. e1332, 2023.
[20] A. Aldahmani, B. Ouni, T. Lestable, and M. Debbah, "Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends," IEEE Open Journal of Vehicular Technology, vol. 4, pp. 281–292, 2023.
[21] H. Alam and E. Tomai, "Security attacks and countermeasures in smart homes," Int. Journal on Cybernetics & Informatics (IJCI), vol. 12, no. 12, p. 109, 2023.
[22] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.
[23] B. K. Sovacool and D. D. F. Del Rio, "Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies," Renewable and Sustainable Energy Reviews, vol. 120, p. 109663, 2020.
[24] R. Faizrakhmanov, A. Platunov, and M. R. Bahrami, "Smart home user interface: Overview," in 2023 Int. Conf. on Industrial Engineering, Applications and Manufacturing (ICIEAM), pp. 595–600, IEEE, 2023.
[25] S. P. Toufighi, J. Vang, A. M. Norouzzadeh, and A. Edalatipour, "Adoption of Internet of Things in residential smart homes: A structural equation modeling approach," Sustainable Futures, vol. 9, p. 100665, 2025.
[26] N. Balta-Ozkan, R. Davidson, M. Bicket, and L. Whitmarsh, "Social barriers to the adoption of smart homes," Energy Policy, vol. 63, pp. 363–374, 2013.
[27] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Benefits and risks of smart home technologies," Energy Policy, vol. 103, pp. 72–83, 2017.
[28] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
[29] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Smart homes and their users: A systematic analysis and key challenges," Personal and Ubiquitous Computing, vol. 19, pp. 463–476, 2015.
[30] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[31] E. Zeng, S. Mare, and F. Roesner, "End user security & privacy concerns with smart homes," in Proc. 13th USENIX Conf. on Usable Privacy and Security (SOUPS), pp. 65–80, 2017.
[32] M. Msgna, "Anatomy of attacks on IoT systems: review of attacks, impacts and countermeasures," Journal of Surveillance, Security and Safety, vol. 3, no. 4, pp. 150–173, 2022.
[33] M. K. Alzaylaee, "A Systematic Review of Security Vulnerabilities in Smart Home Devices and Mitigation Techniques," IJCSNS, vol. 25, no. 3, p. 206, 2025.
[34] N. Fatima, M. Ashraf, R. Tehseen, U. Omer, N. Sabahat, R. Javaid, M. Yousaf, M. Mehr, and A. Zaheer, "AI-powered phishing detection and mitigation for IoT-based smart home security," Journal of Computing & Biomedical Informatics, vol. 8, no. 01, 2024.
[35] D. Buil-Gil, S. Kemp, S. Kuenzel, L. Coventry, S. Zakhary, D. Tilley, and J. Nicholson, "The digital harms of smart home devices: A systematic literature review," Computers in Human Behavior, vol. 145, p. 107770, 2023.
[36] I. Holguin and S. M. Errapotu, "Smart home IoT communication protocols and advances in their security and interoperability," in 2023 7th Cyber Security in Networking Conference (CSNet), pp. 208–211, 2023.
[37] A. Girish, T. Hu, V. Prakash, D. J. Dubois, S. Matic, D. Y. Huang, S. Egelman, J. Reardon, J. Tapiador, D. Choffnes, and N. Vallina-Rodriguez, "In the room where it happens: Characterizing local communication and threats in smart homes," in Proc. 2023 ACM on Internet Measurement Conf. (IMC), pp. 437–456, 2023.
[38] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," Sensors, vol. 18, no. 3, p. 817, 2018.
[39] P. Sutar, S. A. Sarkar, A. Tagare, and A. Pawar, "A review on IoT-enabled smart homes using AI," in 2024 15th Int. Conf. on Computing Communication and Networking Technologies (ICCCNT), pp. 1–6, 2024.
[40] Y. M. Leong, E. H. Lim, and L. K. Lim, "A review of potential AI-based automation for IoT-enabled smart homes," in 2023 IEEE 13th Int. Conf. on System Engineering and Technology (ICSET), pp. 1–6, 2023.
[41] S. Kabir, P. Gope, and S. P. Mohanty, "A security-enabled safety assurance framework for IoT-based smart homes," IEEE Trans. on Industry Applications, vol. 59, no. 1, pp. 6–14, 2022.
[42] M. Kumar, R. K. Gupta, G. Jain, and P. Sharma, "Next-generation smart homes: An IoT approach to home automation and user experience," in 2024 Int. Conf. on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA), pp. 1–6, 2024.

[43] M. Kertous, A. Zerroug, and N. Zerroug, "Review of technics used in smart house," in 2024 2nd Int. Conf. on Electrical Engineering and Automatic Control (ICEEAC), pp. 1–5, 2024.
[44] J. Wang and Y. C. Zhang, "A review on Internet of Things based smart home," in 2021 Int. Conf. on Culture-oriented Science & Technology (ICCST), pp. 273–277, 2021.
[45] A. Adhikary, S. Halder, R. Bose, S. Panja, S. Halder, J. Pratihar, and A. Dey, "Design and implementation of an IoT-based smart home automation system in real world scenario," EAI Endorsed Trans. on Internet of Things, vol. 10, pp. 1–8, 2024.
[46] B. Mustafa, M. W. Iqbal, M. Saeed, A. R. Shafqat, H. Sajjad, and M. R. Naqvi, "IoT based low-cost smart home automation system," in 2021 3rd Int. Congress on Human Computer Interaction, Optimization and Robotic Applications (HORA), pp. 1–6, IEEE, 2021.
[47] P. Franco, J. M. Martinez, Y.-C. Kim, and M. A. Ahmed, "IoT based approach for load monitoring and activity recognition in smart homes," IEEE Access, vol. 9, pp. 45325–45339, 2021.
[48] P. Franco, J. M. Martinez, Y.-C. Kim, and M. A. Ahmed, "A framework for IoT based appliance recognition in smart homes," IEEE Access, vol. 9, pp. 133940–133960, 2021.
[49] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A secure and lightweight authentication protocol for IoT-based smart homes," Sensors, vol. 21, no. 4, p. 1488, 2021.
[50] R. A. Mogbil, M. Alasqah, and S. Elkhediri, "IoT: Security challenges and issues of smart homes/cities," in 2020 Int. Conf. on Computing and Information Technology (ICCIT-1441), pp. 1–6, IEEE, 2020.
[51] K. Vijayaprabakaran, P. Kodidela, and P. Gurram, "IoT based smart intruder detection system for smart homes," Int. J. of Scientific Research in Science and Technology, vol. 8, no. 4, pp. 48–53, 2021.
[52] B. Huang, H. Dong, and A. Bouguettaya, "Conflict detection in IoT-based smart homes," in 2021 IEEE Int. Conf. on Web Services (ICWS), pp. 303–313, IEEE, 2021.
[53] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in Thirteenth Symposium on Usable Privacy and Security (SOUPS), pp. 65–80, 2017.
[54] P. Rashidi and D. J. Cook, "Keeping the resident in the loop: Adapting the smart home to the user," IEEE Trans. on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 39, no. 5, pp. 949–959, 2009.
[55] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT," IEEE Wireless Communications, vol. 23.
[56] C. Bormann, A. P. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," IEEE Internet Computing, vol. 16, no. 2, pp. 62–67, 2012.
[57] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.
[58] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, 2016.
[59] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[60] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The security of IP-based video surveillance systems," Sensors, vol. 20, no. 17, p. 4806, 2020.
[61] L. Schmidt, H. Hosseini, and T. Hupperich, "Assessing the security and privacy of baby monitor apps," Journal of Cybersecurity and Privacy, vol. 3, no. 3, pp. 303–326, 2023.

Authors' Profiles



Tanvir Ahmed is currently pursuing a B.Sc. degree in Internet of Things (IoT) and Robotics Engineering from the University of Frontier Technology, Bangladesh. He is proficient in several programming languages and tools, including Python, C, MATLAB, Arduino, Kotlin, Android Studio, ESP32, and ESP32-CAM, and has hands-on experience with IoT platforms and embedded systems. His research interests include the Internet of Things (IoT), robotics, Artificial Intelligence (AI), Natural Language Processing (NLP), and IoT-based automation.



Md. Akhterujjaman Siddiquee is currently pursuing a B.Sc. degree in Internet of Things (IoT) and Robotics Engineering from the University of Frontier Technology, Bangladesh. He is proficient in several programming languages and tools, including Python, C, MATLAB, Arduino, and TensorFlow, and has hands-on experience with IoT platforms and embedded systems. His research interests include Machine Learning (ML), Artificial Intelligence (AI), the Internet of Things (IoT), robotics, intelligent automation, and related emerging fields. He is particularly passionate about integrating IoT with AI-driven solutions to design smart, adaptive, and efficient systems for real-world applications.



Sheikh Sidratul Muntaha Punno is currently pursuing his BSc student in IoT & Robotics engineering. with hands-on projects—smart navigation for the visually impaired (Flutter, Firebase, generative AI), and Jitsi-based cross-platform video conferencing. RoBERTa and Gemma based student mental-health detection; proficient in Python, C++, Dart/Flutter, Java, and Firebase/Arduino Cloud/Google Drive APIs. Research interests: ML/DL, computer vision, NLP, HCI, CI/CD pipeline, Jenkins, Kubernetes, Docker and smart IoT systems.



Md. Moshiur Rahman obtained his M.Sc. in Software Engineering from the Institute of Information Technology (IIT), University of Dhaka in 2022, and his B.Sc. in Computer Science and Engineering from Patuakhali Science and Technology University (PSTU) in 2019. He worked as a lecturer in the Department of Computer Science and Engineering at Green University of Bangladesh (GUB) from February 2, 2021, to August 30, 2023. Currently, he is a lecturer in the Department of Software Engineering at University of Frontier Technology, Bangladesh (UFTB), starting from January 1, 2024. His research interests include Software Engineering, Machine Learning, Data Science, and Pattern Recognition.



Fahmida Ahmed Antara has been currently employed as Lecturer in the department of IoT and Robotics Engineering, University of Frontier Technology, Bangladesh from 2023. She pursued the Bachelor in Science in Electrical and Electronic Engineering from Rajshahi University of Engineering and Technology in 2016, Masters in Science in Biomedical Physics and Technology from University of Dhaka in 2021. She has experience of 8 years of teaching and conducting research in different universities. Her research interest includes biomedical signal processing, machine learning and electric vehicle technology.



Sadia Enam obtained her M.Sc. in Electrical and Electronic Engineering (EEE) from Rajshahi University of Engineering & Technology (RUET) in 2022, and her B.Sc. was also in EEE from RUET in 2016. She worked as a lecturer in the Department of EEE at North Bengal International University (NBIU) from October 14, 2016 to November 25, 2022, and at Bangladesh Army University of Engineering & Technology from December 1, 2022 to November 30, 2023. Currently, she is a lecturer in the Department of Internet of Things (IoT) and Robotics Engineering (IRE) at University of Frontier Technology, Bangladesh, starting from January 15, 2023.Her research interest includes antenna simulation and propagation and control theory and control applications.

How to cite this paper

Tanvir Ahmed, Akhterujjaman Siddiquee, Sheikh Sidratul Muntaha Punno, Md. Moshiur Rahman, Fahmida Ahmed Antara, Sadia Enam, "IoT-Based Smart Homes: Technologies, Security Risks and Countermeasures", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.18, No.3, pp. 185-202, 2026. DOI:10.5815/ijieeb.2026.03.11