Advances in Networks
2025, Vol. 12, No. 1, pp. 1-18
https://doi.org/10.11648/j.net.20251201.11

Review Article

Securing the Future: A Survey on Smart Home Security in IoT-Integrated Smart Cities

Muhammad Furqan Zia[1, *, †], Maria Siddiqua[2, †], Messaoud Ahmed Ouameur[1], Miloud Bagaa[1], Fadi Al Turjman[3]

[1]Department of Electrical and Computer Engineering, University of Quebec at Trois-Rivières (UQTR), QC, Canada

[2]Department of Artificial Intelligence and Data Science, The National University of Computer and Emerging Sciences (NUCES), Karachi, Pakistan

[3]Department of Information Systems, AI and Robotics Institute, Near East University, Nicosia, Türkiye

Abstract

The rapid growth of urbanization and technological advancements have led to the rise of smart cities and smart homes, where the Internet of Things (IoT) plays a pivotal role. Smart homes enhance energy efficiency, security, and convenience through automated systems and interconnected devices. This survey provides a comprehensive review of smart home architectures, communication technologies, and applications, emphasizing their integration within smart city infrastructures. It explores key components such as sensors, controllers, and cloud-based platforms that enable seamless automation. Additionally, this paper discusses major challenges in smart home security, including privacy risks, cyber threats, and interoperability issues among IoT devices. Security concerns such as unauthorized access, data breaches, and denial-of-service attacks are analyzed, alongside strategies to mitigate these risks. The study also highlights the importance of secure communication protocols, authentication mechanisms, and encryption techniques to ensure the resilience of smart home systems. Furthermore, this survey examines emerging research directions in smart home technology, including AI-driven automation, energy-efficient systems, and blockchain-based security solutions. As smart homes continue to evolve, addressing these challenges will be crucial for their widespread adoption. This paper aims to serve as a valuable resource for researchers, developers, and policymakers seeking to enhance the security and functionality of smart homes within the broader framework of smart cities.

Keywords

Smart Home, IoT Security, Home Automation, Communication Technologies, Secure Smart Homes

1. Introduction

The proportion of the global population living in cities has surpassed 50% and is projected to reach 70% by 2050 [1]. This rapid urbanization has intensified the demand for efficient resource management, improved governance, and enhanced quality of life. To address these challenges, the concept of smart cities has emerged, leveraging advancements in

[*]Corresponding author: Muhammad.Furqan.Zia@uqtr.ca (Muhammad Furqan Zia)

[†]MuhammadFurqanZia and MariaSiddiqua are co-first authors.

Received: 17 February 2025; **Accepted:** 28 February 2025; **Published:** 21 March 2025

information and communication technologies (ICT). A smart city is a self-sustaining ecosystem that integrates advanced technologies such as IoT, sensors, base stations, and communication protocols, all managed through sophisticated databases and algorithms [2]. At the core of a smart city lies the concept of smart homes, which are residential units equipped with advanced technologies to automate and optimize daily operations, ensuring energy efficiency, security, and convenience.

Smart homes are revolutionizing traditional living spaces by incorporating IoT-enabled devices such as cameras, motion sensors, fire alarms, and smart appliances. These devices collect and analyze data to automate tasks, reducing the need for humanintervention. For instance, a smart home can adjust lighting, temperature, and security systems based on real-time data, ensuring optimal functionality and energy savings [3]. The integration of smart homes into smart cities has led to the development of various applications, including smart grids, smart meters, water management systems, healthcare monitoring, and surveillance systems [4]. These applications aim to enhance resource utilization, improve governance, and provide better services to urban residents.

Despite the significant progress in smart home technologies, several challenges remain, particularly in the areas of security, privacy, and interoperability. Researchers and industry experts are actively working to address these issues to ensure the safe and efficient deployment of smart homes in smart cities. As smart homes become more connected through IoT-based wireless networks, they also become more vulnerable to security threats. Traditional security methods often fall short in addressing evolving risks like unauthorized access, eavesdropping, and denial-of-service (DoS) attacks. Similar concerns have been observed in cognitive radio networks, where dynamic spectrum access and decentralized communication make secure transmissions more challenging [44]. Meanwhile, research on next-generation Wi-Fi and multi-user downlink frameworks indicates that incorporating non-orthogonal signaling can strengthen security and resilience in smart home networks [45]. To protect IoT-integrated smart homes within smart cities, there is a growing need for advanced security frameworks that utilize physical layer security (PLS), multi-carrier transmission, and AI-driven threat detection.

However, In this survey we focuses on the automation of smart homes within the broader context of smart cities. It provides a comprehensive analysis of the architectures, devices, communication technologies, and techniques used in smart home systems. Additionally, the paper highlights the challenges and open research issues in this domain, offering insights into future directions for secure and efficient smart home deployment.

The paper is organized into several sections to provide a structured overview of the topic. Section 2 discusses the background, objectives, and constraints of smart homes in smart cities. Section 3 explores existing and emerging applications of smart home technologies. The architecture and fundamental components of smart homes, along with trustworthy computing models, are detailed in Sections 4 and 5. Section 6 categorizes the devices used in smart homes, while Section 7 and 8 explain secure deployment strategies and wireless communication protocols, respectively. Section 9 addresses critical challenges such as security and privacy, along with potential countermeasures. Section 10 provides insights into the deployment of smart homes, and Section 11 identifies open research issues to guide future studies. Finally, Section 12 concludes the paper by summarizing the key findings and their implications for the future of smart homes in smart cities.

This paper aims to serve as a valuable resource for researchers and practitioners seeking a unified understanding of secure smart homes in the context of smart cities. By covering a wide range of aspects, this survey paper contributes to the ongoing efforts to create smarter, safer, and more sustainable urban living environments.

Figure 1. *Paper Organization.*

2. Background

As urban populations continue to grow, cities face significant challenges in resource management, infrastructure sus-

tainability, and disaster resilience. Addressing these challenges is crucial to enhancing the quality of life for citizens. One of the most promising solutions is the development of smart cities, which leverage advanced technologies to create more efficient, sustainable, and adaptable urban environments.

Smart cities integrate wireless technologies to optimize resource utilization and improve disaster preparedness. Ensuring secure communication is a key challenge in integrating smart homes into smart cities. Wireless technologies like Wi-Fi, LTE, and ZigBee are essential for device-to-device communication, but they remain susceptible to threats such as eavesdropping, data interception, and authentication breaches. Recent developments in non-orthogonal multiple access (NOMA) offer a new approach to secure wireless transmission, enabling multi-user and multi-cell communication that helps prevent unauthorized access while optimizing resource allocation [46]. Additionally, physical layer security (PLS) methods—such as interference-based encryption and pre-coded multi-antenna transmission have shown promising results in countering security risks in IoT-enabled smart devices [47]. Integrating PLS into future smart home networks could significantly strengthen their defense against cyber threats, making them more resilient and secure [48].

Wireless communication facilitates seamless connectivity among various urban components, such as smart grids, intelligent transportation systems, automated surveillance, and environmental monitoring. These interconnected systems enhance efficiency, reduce costs, and provide better solutions for managing urban infrastructure.

A smart city, along with smart homes, relies on essential components such as smartphones, sensors, and networks to function effectively in a wireless and mobile environment. Sensors play a crucial role in monitoring and supporting infrastructure, including smart grids, home automation, surveillance systems, vehicular navigation, and even earthquake detection in buildings. The deployment of wireless networks enables real-time communication among these devices, ensuring better decision-making and automated responses to various urban challenges.

Wireless networks use radio waves as the primary communication medium, offering advantages such as flexibility, cost-effectiveness, and ease of deployment. Several types of networks are utilized in smart city applications, each with unique advantages. These include Local Area Networks (LAN), Wide Area Networks (WAN), Metropolitan Area Networks (MAN), WiMAX, Wi-Fi, and Zigbee. Each of these technologies plays a critical role in enabling smart city functionalities and ensuring seamless communication across various components of the ecosystem.

Objectives: The primary objective of research in smart cities and smart homes is to develop and deploy cost-efficient, high-performance infrastructure. Key research studies have explored various aspects of smart home automation and security:

1) In [7], researchers focused on building cost-effective smart homes with enhanced security features.
2) In [8], different automation techniques were examined, such as control via web browsers, cloud servers, GSM, and Bluetooth.
3) In [9], security challenges in smart homes were analyzed, including authentication, integration, and standardization issues.
4) In [10], a mobile application was proposed to control multiple home appliances remotely using IoT, providing flexibility and improved security.
5) In [11], various home automation methodologies were discussed, highlighting innovations in automation frameworks.

The proposed smart home and city frameworks aim to offer greater automation flexibility, improved security, and enhanced management solutions for water conservation and child safety.

Constraints: Despite the advancements in smart city and home automation technologies, several constraints hinder widespread implementation. Key challenges identified in literature include:

1) *Cost Efficiency:* Studies such as [7] emphasize the high cost of smart home deployment, including equipment, installation, wiring, and development expenses. Researchers explore methods to reduce these costs while maintaining performance.
2) *Internet Connectivity:* In [8], challenges in maintaining a stable internet connection, particularly in rural areas, are highlighted. Continuous internet access is necessary for cloud-based smart home solutions, posing a barrier in low-connectivity regions.
3) *Security Concerns:* Research in [9] discusses issues related to controlling multiple devices simultaneously, ensuring data security, and addressing integration challenges within smart homes.
4) *Communication Efficiency:* In [11], various communication techniques were evaluated based on cost, efficiency, and data transmission rates.
5) *System Vulnerabilities:* Security concerns related to smart home automation systems were elaborated in [12], emphasizing the potential threats that could compromise the functionality of connected devices.

The following table summarizes key constraints associated with smart home implementations across different research studies.

Table 1. *Comparison of smart homes constraints for different metrics.*

Reference	Technology	Energy	Control	Cost	Efficiency	Security	Connectivity	Speed	Performance
7	Yes	Yes	No	Yes	No	Yes	No	No	No
8	Yes	No	No	Yes	No	No	Yes	Yes	No
9	No	No	Yes	No	Yes	Yes	No	No	No
10	Yes	No	No	Yes	Yes	No	No	Yes	Yes
12	No	No	No	Yes	Yes	Yes	No	No	Yes

3. Applications of Smart Homes

In recent years, engineers and researchers have made significant strides in developing innovative applications for smart homes. These applications leverage a variety of sensors such as motion, light, fire, and environmental sensors to detect activities and gather data. The collected information is then processed to trigger appropriate actions, enhancing convenience, security, and energy efficiency. Below is an in-depth exploration of the key applications currently being utilized in smart homes:

1) Smart Lighting

Smart lighting systems are revolutionizing the way we interact with lighting in our homes. These systems require smart bulbs, motion sensors, light sensors, and a wireless connection to enable control via mobile applications. Users can manage their lighting remotely through internet or Bluetooth connections. Additionally, motion and light sensors automate lighting control by adjusting brightness or turning lights on/off based on occupancy and ambient light levels. For instance, lights can dim during the day when natural light is sufficient or turn on automatically when someone enters a room. Research by [13] provides a detailed analysis of lighting control systems in smart homes, highlighting their energy-saving potential and user convenience.

2) Smart Garage

The smart garage is a cornerstone of modern home automation, with its primary functionality being the automated garage door opener. These systems often employ rolling-code technology, such as the KeeLoq lightweight block cipher, to generate secure, cryptographically encoded signals. When a user syncs their remote control with the garage door opener, both devices generate matching codes in the same sequence, ensuring secure access. Advanced systems also integrate with mobile apps, allowing users to monitor and control their garage doors remotely. In [14], the author delves into the security measures and operational functionalities of smart garage systems, emphasizing their role in enhancing home security.

3) Smart Meters

Smart meters are fundamental to energy management in smart homes. These devices provide real-time monitoring and control over energy-consuming units within the home. A typical smart meter consists of three main sections:

a. *Base Station:* Includes components like IoT gateways, appliance trackers, and data repositories.
b. *Appliance Controller:* Equipped with sensors and relay modules to manage connected devices.
c. *User Interface:* Allows homeowners to monitor energy consumption patterns and optimize usage.

By providing detailed insights into energy usage, smart meters empower users to reduce waste and lower utility bills. Reference [15] offers a comprehensive explanation of smart meter functionality and their role in promoting sustainable energy practices.

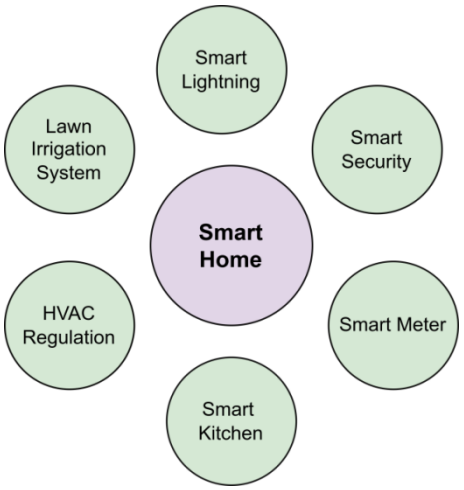

Figure 2. *Applications of smart home.*

4) Smart Kitchen

The kitchen is a focal point of smart home automation, with a wide range of intelligent appliances designed to simplify daily tasks. For example:

a. *Smart Refrigerators:* Devices like LG's Smart ThinQ can scan grocery receipts, track inventory, and send alerts when items are nearing expiration. They can also suggest recipes based on available ingredients.

b. *Energy Monitoring:* By automating kitchen appliances and accessing them via smartphones, users can monitor energy consumption and reduce waste.

These innovations not only enhance convenience but also contribute to energy efficiency and sustainability. Reference [16] explores the integration of smart kitchen appliances and their impact on modern living.

5) HVAC Regulation

Heating, ventilation, and air conditioning (HVAC) systems account for nearly 50% of a home's annual energy costs. Smart HVAC systems optimize energy usage by adjusting temperatures based on occupancy and user schedules. For instance, the system can lower heating or cooling when a room is unoccupied and restore comfort levels before occupants return. Advanced systems also integrate weather forecasts to further enhance efficiency. Reference [16] discusses the benefits of automated HVAC systems in reducing energy consumption and improving home comfort.

6) Lawn Irrigation Systems

Maintaining a lush and healthy lawn can be challenging, especially with unpredictable weather conditions. Traditional sprinkler systems often waste significant amounts of water due to inefficiencies. Smart irrigation systems, such as Skydrop, address this issue by leveraging real-time weather data to optimize watering schedules. For example, if rainfall provides sufficient moisture, the system will automatically disable scheduled watering, conserving water and reducing costs. In [16], the authors highlight the environmental and economic benefits of smart lawn irrigation systems.

7) Smart Security

Home security is a top priority for homeowners, and smart security systems offer advanced solutions to safeguard properties. These systems typically include:

a. *CCTV Cameras:* Provide real-time surveillance and recording.
b. *Motion Sensors:* Detect unauthorized movement and trigger alarms.
c. *Biometric Devices:* Enable secure access through fingerprint or facial recognition.
d. *Automated Alerts:* Notify homeowners and authorities in case of a security breach.

By integrating these components, smart security systems provide robust protection and peace of mind. Reference [16] explores the latest advancements in home security technologies and their effectiveness in deterring intruders.

8) Emerging Applications

Beyond the applications mentioned above, smart home technology continues to evolve, introducing new possibilities such as:

1) *Smart Health Monitoring:* Integration of wearable devices and health sensors to track residents' well-being.
2) *Voice-Activated Assistants:* Systems like Amazon Alexa and Google Home enable hands-free control of various smart devices.
3) *Energy Storage Systems:* Integration with solar panels and home batteries to optimize energy usage and reduce reliance on the grid.

In the forthcoming section, we will delve into the architecture and core components of smart homes, providing a deeper understanding of how these systems are designed and integrated.

4. Architecture and Main Components

Smart home systems comprise several essential components, including sensors, actuators, wireless signal control devices, appliances, and monitoring systems. Sensors play a crucial role in detecting various activities such as light intensity, motion, and temperature. Actuators are responsible for executing mechanical movements and controlling various home automation mechanisms. These actuators require a power source and a controlled signal to function efficiently. Wireless signal control devices, such as modems, facilitate seamless communication between different components. Additionally, smart appliances like refrigerators, air conditioners, and washing machines enhance convenience, while surveillance devices such as cameras and monitoring screens improve security.

Various architectural models have been proposed for smart home implementation within smart cities. Among these, researchers widely recommend a three-layered architecture for smart home automation [17]. This model comprises:

1) *Sensing Layer*
2) *Network Layer*
3) *Application Layer*

Each of these layers plays a critical role in the overall functionality of a smart home system.

1) Sensing Layer

The sensing layer is responsible for collecting data from different home appliances and environmental conditions within a household. Sensors embedded in appliances, doors, and other household items gather data on temperature, light, motion, and other factors. These sensors transmit data to microprocessors such as the SAMSUNG S3C2440A, which process and forward the information. Wireless modules like ZigBee [9] enable communication between the sensing layer and the next stage in the architecture.

2) Network Layer

The network layer serves as an intermediary, gathering data from the sensing layer via wireless communication technologies such as Wi-Fi and ZigBee. It efficiently transfers the collected data to the application layer while employing various network protocols to ensure optimal data transmission. This layer acts as a bridge, facilitating seamless data exchange between lower and upper layers.

3) Application Layer

The application layer, the topmost layer in this architecture, receives data from the network layer and utilizes it for various automation purposes. Typically, applications installed on smart phones allow users to control home appliances remotely.

Notable smart home applications include Nest and Samsung SmartThings [18]. Users can leverage these applications to manage home settings wirelessly, enhancing convenience and energy efficiency.

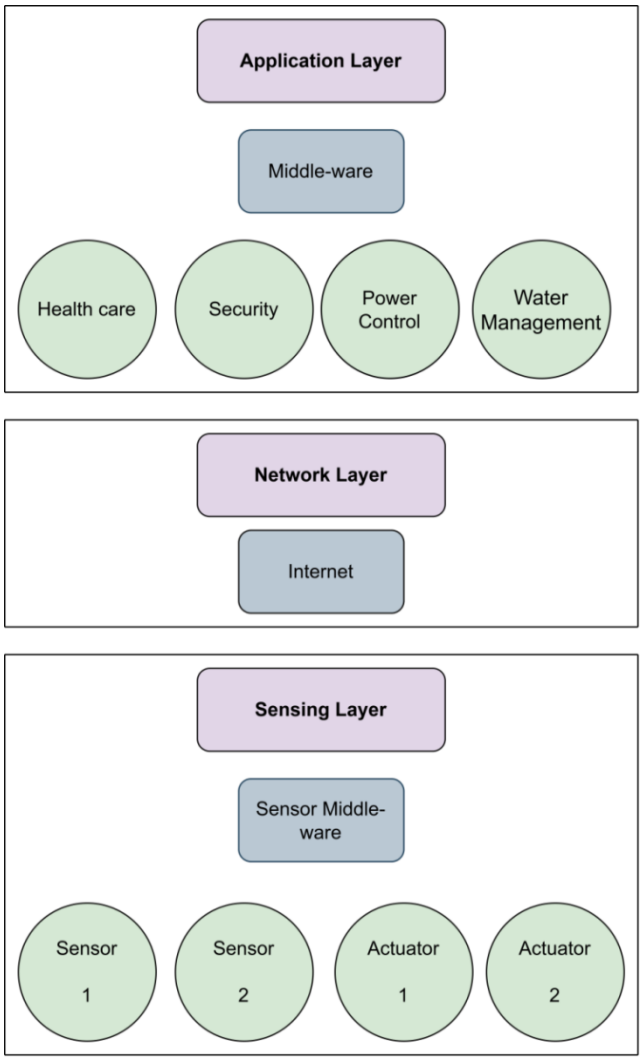

Figure 3. *Architecture and components in smart homes.*

5. Trustworthy Computing Models

As smart home technologies continue to evolve, ensuring security, privacy, and reliability has become a pressing challenge. Cyber threats targeting IoT ecosystems are growing in complexity, making it essential to adopt robust computing models that safeguard data integrity and enable seamless device interoperability. To address these concerns, modern security frameworks integrate AI-driven trust management, blockchain-based authentication, physical layer security (PLS), and decentralized access control mechanisms [49].

1. AI-Driven Trust Management

Artificial intelligence plays a crucial role in enhancing the security of smart homes by enabling real-time intrusion detection, anomaly identification, and automated threat mitigation. Machine learning (ML) models help [50]:

1) Detect compromised devices by analyzing behavioral patterns and identifying suspicious network activity.
2) Predict potential cyber threats using deep learning and federated learning techniques while maintaining user privacy.
3) Automate authentication processes and dynamically adjust security policies based on real-time threat assessments.

Federated learning, in particular, allows multiple smart home networks to collaborate on security threat detection without directly sharing sensitive data, improving overall system resilience.

2. Blockchain-Based Secure Authentication

Blockchain technology is increasingly being used to establish decentralized, tamper-proof authentication methods for IoT devices. Key benefits include [51]:

1) Decentralized Identity Management (DID): Each IoT device is assigned a cryptographic identity, preventing unauthorized access.
2) Tamper-Proof Security Logs: Immutable records of security events enable forensic analysis and fraud detection.
3) Smart Contract-Based Access Control: Security policies are enforced automatically without relying on centralized control.

To address concerns about energy efficiency, lightweight blockchain mechanisms such as Delegated Proof-of-Stake (DPoS) and Directed Acyclic Graphs (DAGs) offer reduced power consumption, making them suitable for smart home environments.

3. Physical Layer Security (PLS) for Smart Homes

PLS enhances security by leveraging wireless transmission characteristics to prevent eavesdropping and unauthorized data interception. Some notable PLS techniques include [52]:

1) Dynamic Encryption: Secret keys are generated based on radio channel variations, eliminating the need for traditional cryptographic exchanges.
2) Artificial Noise (AN) Jamming: Interference is introduced to disrupt unauthorized receivers while allowing legitimate users to recover the original signal.
3) Adaptive Beamforming & Reconfigurable Intelligent Surfaces (RIS): These technologies create secure transmission paths, reducing the risk of signal interception.

Recent studies show that combining PLS with AI-driven channel estimation strengthens protection against man-in-the-middle (MITM) attacks, improving overall network security.

4. Trustworthy Edge Computing for IoT Security

With the increasing reliance on edge computing in smart homes, security measures must be implemented at the edge layer rather than solely in the cloud. Edge-based security enhances [53]:

1) Low-Latency Authentication:IoT devices are verified

locally before accessing cloud services.

2) Real-Time Anomaly Detection: Security threats are identified and mitigated at edge nodes before spreading across the network.
3) Self-Adaptive Security Policies: AI-powered edge systems continuously learn from emerging threats and update security protocols dynamically.

Integrating Zero Trust Architecture (ZTA) in smart home networks ensures that all device interactions are continuously verified, preventing unauthorized access even from previously trusted devices.

5. Reputation-Based Trust Models for IoT Devices

Reputation-based security models assign trust scores to smart home devices based on their historical behavior, compliance with security policies, and peer evaluations. These models help [54]:

1) Identify rogue devices attempting unauthorized access.
2) Mitigate data poisoning attacks that could compromise smart home automation systems.
3) Enable dynamic access control by restricting devices with low trust scores from accessing critical resources.

By combining AI-driven anomaly detection, blockchain-based verification, and PLS-enhanced communication security, smart home networks can achieve a multi-layered, adaptive security framework that evolves to counter emerging cyber threats.

This holistic approach to cybersecurity ensures that IoT-integrated smart homes remain resilient, protecting user data and maintaining seamless connectivity in the evolving digital landscape.

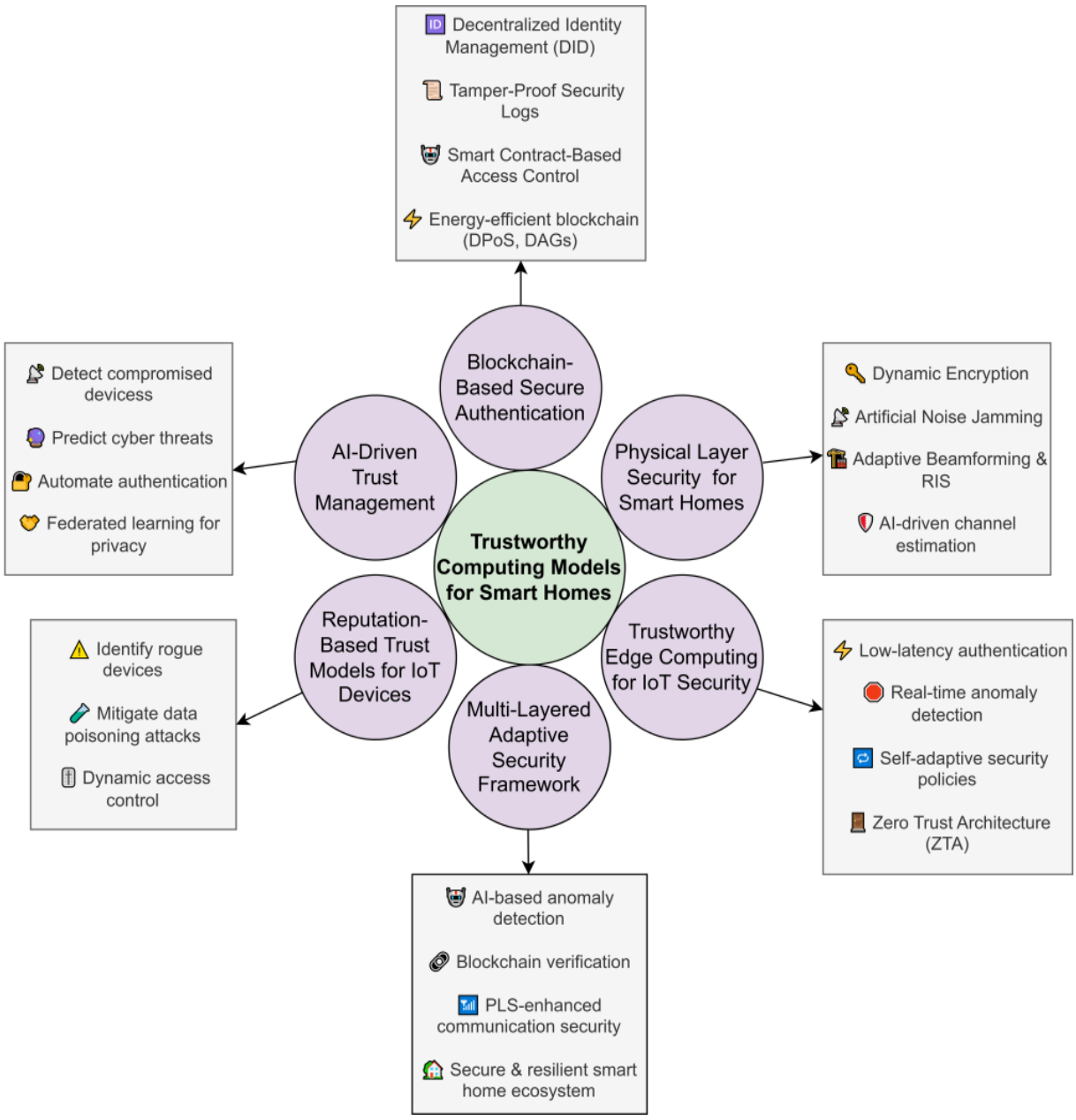

Figure 4. *Trustworthy Computing Models for Smart Homes.*

6. Techniques Used in Home Automation

Several techniques have been explored in the literature to enhance smart home automation, improving the efficiency and connectivity of home devices. These techniques can be broadly categorized into two main approaches:

a. Voice Recognition-Based Home Automation

b. IoT-Based Home Automation [19].

Voice Recognition-Based Home Automation

A voice recognition-based home automation system was proposed and implemented by researchers [20]. The hardware setup includes an Arduino UNO microcontroller and a smartphone. Wireless communication between Arduino and smartphones are established using Bluetooth. Smartphones utilize built-in voice recognition commands, enabling users to control home appliances via voice input [11]. Furthermore, Android devices use Google Assistant, while iOS devices employ Siri for voice-controlled automation.

IoT-Based Home Automation

A study [21] introduced a home control and monitoring system based on IoT technology. The system was designed and implemented using an embedded micro-web server, controlling devices, and a smart home software application. The proposed architecture consists of three key components:

a. *Home Environment:* Contains hardware interface modules and a home gateway to manage smart devices.

b. *Home Gateway:* Acts as a bridge between the home environment and external networks.

c. *Remote Environment:* Enables authorized users to monitor and control home appliances remotely via smartphones using Wi-Fi, 3G, or 4G networks.

Table 2. *Comparison between home automation control techniques.*

Technology	Cost	Efficiency	Flexibility	Response
Voice Recognition	Moderate	Moderate	High	Moderate
IoT Based	High	High	High	High

7. Devices Used in Smart Homes

A wide range of devices are utilized in home automation to enhance convenience, security, and overall quality of life. These devices can be categorized as follows:

1) Sensing Devices

Smart homes incorporate various sensors designed to monitor and respond to environmental changes. These include:

a. *Fire Sensors:* Detect smoke or fire and activate water sprinklers for fire suppression.

b. *Moisture Sensors:* Identify moisture levels in walls, helping to prevent water damage and mold growth.

c. *Motion Detectors:* Detect movement within the home and can trigger lighting or security alerts.

d. *Light Sensors:* Measure ambient light levels and automatically turn lights on or off as needed.

e. *Water Sensors:* Monitor water levels in tanks and help prevent overflow or shortages.

f. *Pressure Sensors:* Detect pressure variations inside and outside the home, providing valuable data for home automtion systems.

g. *Gas Sensors:* Identify the presence of harmful gases, such as carbon monoxide or natural gas leaks, and trigger alerts for safety.

h. *Other Sensors:* These include chemical sensors for detecting hazardous substances and thermostat sensors for climate control.

2) Appliances

Smart home automation extends to various household appliances, improving efficiency and convenience across different areas of the home:

a. *Kitchen Appliances:* Refrigerators, kettles, juicers, microwaves, blenders, and cookers.

b. *Washroom Appliances:* Washing machines, hand dryers, and toilet roll dispensers.

c. *Living Room Appliances:* Air conditioners, fans, lights, and heaters.

3) Entertainment Devices

Smart homes integrate entertainment systems for leisure and recreation, including:

a. *Home Theater Systems:* Smart TVs, DVD players, and high-quality speakers.

b. *Gaming Devices:* Computers, monitors, gaming consoles such as Xbox and PlayStation.

c. *Music Devices:* Smart speakers, sound systems, and microphones for immersive audio experiences.

4) Security Devices

Security is a fundamental aspect of smart homes, with various devices ensuring the safety of occupants:

a. *CCTV Cameras:* Provide real-time surveillance and remote monitoring.

b. *Alarms:* Trigger alerts in case of unauthorized access or

emergencies.

c. *Monitoring Screens:* Display live feeds from security cameras for enhanced surveillance.

By integrating these devices, smart homes offer a seamless, automated, and secure living environment, improving both comfort and safety.

Table 3. *Categories of devices in home automation.*

Categories	Devices
SensingDevices	Fire, Moisture, Motion, Light, Water
Appliances	Kitchen: (Refrigerators, Kettles, Juicers, Microwave). Washroom: (Washing Machines, Hand Dryers, Toilet Roll Dispensers). Living Room: (Air Conditioners, Fans, Lights, Heaters).
Entertainment Devices	Home Theater Devices: (TVs, DVD Box, Speakers). Gaming Devices: (Computers, Monitors, Xbox, PlayStation). Music devices: (Speakers, Microphones).
SecurityDevices	CCTV Cameras, Alarms and monitoring screens

8. Security in Smart Homes

Security in smart homes is not just a technical concern it's a fundamental requirement for protecting personal data, ensuring privacy, and maintaining the reliability of automated systems. As smart home devices become more interconnected, they also become more vulnerable to cyber threats like unauthorized access, data breaches, and denial-of-service (DoS) attacks. To counter these risks, robust security frameworks must be in place, starting with strong user and device authentication to prevent unauthorized entities from infiltrating the system [5]. Secure communication protocols, such as end-to-end encryption and network monitoring tools, are essential for detecting and blocking malicious activities before they compromise sensitive data [6]. Moreover, integrity measures, such as message authentication codes (MAC), help ensure that data remains unaltered during transmission. To enhance resilience, smart home networks should integrate real-time anomaly detection systems, which use AI to recognize suspicious behavior and take immediate action. Finally, Zero Trust Architecture (ZTA) is becoming a critical defense mechanism, requiring continuous verification of all devices and users to prevent unauthorized access even from previously trusted sources. By addressing these security and privacy concerns proactively, smart home environments can remain secure, reliable, and efficient, offering both peace of mind and seamless automation for homeowners [37].

8.1. Security and Privacy Requirements for Smart Home Services

The security of smart homes is a crucial aspect that directly impacts user privacy and system reliability. While smart home technologies offer convenience and automation, ensuring their protection against potential threats remains a primary concern. To establish a secure environment, certain fundamental security measures must be implemented.

Existing research has identified several key security and privacy requirements essential for smart homes. For instance, [40] outlines critical aspects such as data confidentiality, data integrity, and device-to-device authentication. Broadly, security and privacy concerns can be categorized into three main principles: confidentiality, integrity, and availability. Addressing these aspects strengthens the overall security framework of smart home systems, mitigating risks associated with unauthorized access, data breaches, and cyber attacks.

The Table 4 below summarizes some of the fundamental security requirements for smart home environments.

Table 4. *Security and privacy requirements for smart home.*

Category	Security Requirement
User and Device Authentication	In a smart home, numerous devices are interconnected and rely on the internet for software updates, security patches, and data exchange. Only authorized users should be allowed to perform these functions. A robust authentication mechanism or key management technique is necessary to prevent unauthorized devices and users from gaining access. Without such techniques, it is impossible to protect the smart home from adversaries [40, 41].

Category	Security Requirement
Network Monitoring	In a smart home, various entities such as home appliances, Energy Storage Systems (ESS), and Renewable Energy Sources (RES) are connected to the network. Adversaries can target the smart home network via Denial of Service (DoS) attacks and other network-based threats. To defend against such attacks, it is essential to install monitoring and intrusion detection tools. Without these tools, it is not possible to secure the network from these types of threats.
Integrity	Integrity ensures that information cannot be altered by unauthorized users during any process, whether it's message requests, storage, or transmission. Data must remain unaltered and intact at all stages. In other words, integrity guarantees that information is transmitted accurately and consistently. Adversaries often compromise integrity through malicious software attacks [42]. Message Authentication Codes (MAC) are commonly used to verify integrity.
Availability	Availability guarantees that network services and resources remain accessible at all times while being protected from malicious attacks. In the context of smart homes, malicious threats and DoS attacks can disrupt or expose network services and resources. Disaster recovery solutions are essential for ensuring the continued availability of services within the smart home network [41].
Confidentiality	Confidentiality ensures that users' private information remains secure and is only accessible by authorized individuals. Cryptography and effective key management strategies are employed to maintain confidentiality and protect user data from unauthorized access [43].

8.1.1. Security Challenges

As smart homes and IoT ecosystems continue to evolve, they face numerous security threats that can compromise user data, disrupt services, and expose sensitive information to cybercriminals. Addressing these challenges requires a combination of robust authentication mechanisms, encryption protocols, and proactive cybersecurity measures. Below are some of the most pressing security concerns in IoT-integrated smart environments:

1) Authentication Vulnerabilities

Authentication plays a critical role in verifying the identities of users and devices in a network. Unauthorized access to servers containing sensitive data can lead to data breaches, identity theft, and unauthorized system modifications. Strong authentication measures such as multi-factor authentication (MFA), biometric verification, and randomly generated captchas can significantly reduce the risk of unauthorized access [29].

2) Man-in-the-Middle (MitM) Attacks

In MitM attacks, a cybercriminal intercepts and manipulates communication between two systems without their knowledge. For instance, an attacker could alter temperature sensor data in a smart home system, misleading automation decisions. End-to-end encryption, secure authentication protocols, and digital certificates are effective countermeasures against such attacks, ensuring data integrity and confidentiality.

3) Data and Identity Theft

IoT devices such as wearables, smart locks, and home assistants often store and transmit personal information. If these devices lack proper security, hackers can steal sensitive data for fraudulent transactions, identity theft, or black-market sale. To protect user information, data encryption, secure cloud storage, restricted data sharing, and strong password policies must be implemented [30].

4) Masquerading Attacks

Masquerading attacks occur when a malicious entity impersonates a legitimate device or system using stolen credentials or public keys. This technique is often used in combination with phishing scams and credential theft to gain unauthorized access. To counter such threats, multi-step identity verification, certificate-based authentication, and behavioral monitoring should be employed.

5) Eavesdropping on Communications

Eavesdropping is a passive cyberattack in which an unauthorized party listens in on communication channels, such as phone calls, messages, or real-time data transfers. Attackers exploit unsecured networks to steal credentials, sensitive conversations, and personal data. The most effective way to prevent this is through end-to-end encryption (E2EE), VPN usage, and secure Wi-Fi configurations [45].

6) Device Hijacking

Device hijacking occurs when an attacker gains unauthorized control over a smart device, allowing them to manipulate its functions without the owner's knowledge. Since hijacked devices often continue to operate normally, users may not immediately notice the compromise. A compromised thermostat, security camera, or door lock can provide access to other networked devices, potentially leading to complete home automation takeovers. To prevent hijacking, regular firmware updates, strong passwords, and intrusion detection systems should be used [31].

7) Distributed Denial of Service (DDoS) Attacks

A Denial of Service (DoS) attack overwhelms a device or network resource, making it unavailable to legitimate users. In a DDoS attack, multiple compromised devices often part of a botnet are used to launch large-scale disruptions. IoT devices with weak security settings can be hijacked and used in such attacks. Effective anti-DDoS solutions, firewall configura-

tions, and DNS protection mechanisms are necessary to prevent these threats [22].

8) Permanent Denial of Service (PDoS) Attacks

Unlike standard DDoS attacks, Permanent Denial of Service (PDoS) aims to irreversibly damage or disable a device, often requiring hardware replacement. Attacks such as BrickerBot exploit factory-default credentials and firmware vulnerabilities to corrupt device functionality permanently. To mitigate such risks, firewall hardening, intrusion prevention systems (IPS), and regular device audits should be implemented [23].

9) False Information Attacks

In this type of attack, cybercriminals deliberately introduce misleading or manipulated data into a network, causing devices to make incorrect decisions. For example, tampering with smart energy meters could result in inflated electricity bills, or fake sensor data could lead to incorrect automation triggers. Implementing data validation protocols, AI-based anomaly detection, and blockchain-based verification can help prevent false information attacks [32].

8.1.2. Security Countermeasures

To effectively protect smart home devices from cyber threats, a comprehensive IoT security framework must be implemented, covering device-to-cloud security without compromising the profitability or time-to-market for service providers and manufacturers. A well-structured security strategy should integrate the following key countermeasures:

1) Secure Boot Mechanism

Secure boot ensures that IoT devices only run authentic and trusted firmware by verifying digital signatures before executing code. This technique prevents attackers from injecting malicious firmware or unauthorized modifications into the device's operating system. By using cryptographic code-signing methods, manufacturers can ensure that only firmware updates signed by the Original Equipment Manufacturer (OEM) or a trusted third party are installed. Implementing secure boot helps maintain system integrity and protects against firmware-based malware attacks [55].

2) Mutual Authentication for Device Verification

Before transmitting or receiving data, smart home devices must undergo mutual authentication to verify their legitimacy within the network. This prevents attackers from injecting fake or compromised devices into the system. Cryptographic techniques such as the Secure Hash Algorithm (SHA) and Digital Signature Algorithm (DSA) play a crucial role in establishing a secure two-way authentication process, ensuring that both the sender and receiver can trust each other's identities. Implementing Public Key Infrastructure (PKI) can further enhance the authentication mechanism by using digital certificates [56].

3) Secure Communication with End-to-End Encryption

Encrypting data in transit between smart home devices and the cloud prevents unauthorized interception and ensures that only legitimate users can access sensitive information. Encryption methods such as AES-256 (Advanced Encryption Standard) and Transport Layer Security (TLS) secure communication between IoT devices, cloud platforms, and mobile applications. For example, when a smart thermostat sends operational data to a cloud server, end-to-end encryption ensures that cybercriminals cannot intercept, modify, or manipulate the transmitted information [57].

4) Continuous Security Monitoring & Threat Detection

To detect and respond to cyber threats in real-time, comprehensive security monitoring should be implemented across the IoT ecosystem. This includes [58]:

1. Capturing security logs from endpoint devices and network traffic.
2. Identifying abnormal patterns, such as unauthorized access attempts or data manipulation.
3. Triggering automated security responses to block potential cyber attacks.

Advanced Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can help analyze security threats dynamically and mitigate attacks before they cause significant damage. Real-time monitoring enables immediate response to cyber incidents, ensuring that security breaches are contained swiftly.

5) Security Lifecycle Management & Secure Decommissioning

Security should not only focus on active devices but also consider the entire device lifecycle, from deployment to decommissioning. Lifecycle management helps manufacturers and service providers maintain security throughout the operational life of an IoT device. This includes [59]:

Over-the-Air (OTA) security updates, allowing immediate patching of vulnerabilities.

Device key management, ensuring encryption keys are securely replaced if compromised.

Secure device decommissioning, preventing discarded devices from being repurposed for malicious use.

By securely managing device lifecycle operations, cybercriminals cannot exploit old or retired IoT devices to gain access to a network.

8.2. Secure Deployment of Smart Devices

Ensuring the secure deployment of smart home devices is a major concern today. With the increasing number of security threats, it is essential to implement proper security measures when deploying these devices. Several techniques and parameters should be considered to enhance the security of smart home systems.

1) Device Reviews and Research

Before purchasing a smart home device, users should conduct thorough research and read reviews to assess its security and performance. Reviews can provide insights into whether a device has been previously targeted by hackers and how well it withstands cyber threats. A well-reviewed device with a strong security track record is less likely to be vul-

nerable to attacks.

2) Secure Connection Applications

It is crucial to verify the application that connects smart home devices. Users should check:

a. The developer or company behind the application.
b. The app's security rating and reviews.
c. Whether the application receives regular updates to enhance security.

A well-maintained application with frequent updates is more likely to incorporate the latest security features, reducing the risk of vulnerabilities.

3) Password Protection

Most modern smart home devices support password protection. However, users should ensure that the device allows them to change the default password. Some manufacturers restrict password modifications, which increases security risks by making devices more vulnerable to attacks. Always opt for devices that allow customizable, strong passwords.

4) Two-Factor Authentication (2FA)

Two-factor authentication (2FA) provides an additional layer of security by requiring two types of credentials for authentication. Typically, one factor is a physical validation token (e.g., a smart card or biometric scan), while the other is a logical code or password. Enabling 2FA significantly reduces the risk of unauthorized access.

5) Device Preparation and Authentication

Before integration into a smart home system, devices must undergo a secure setup process. This includes:

a. Scanning the QR code on the device or selecting the correct product title from the app.
b. The app retrieving a product_uuid and sending it to the cloud.
c. The app broadcasting a PT_SCAN message containing the product_uuid and the application's EC public key.
d. The application prompting the user to input Wi-Fi credentials and initiating Wi-Fi provisioning.

6) Secure Wi-Fi Provisioning

During the Wi-Fi setup of a headless IoT device, several common methods are used, such as Access Point Mode, Wi-Fi Direct, and TI's SmartConfig. JoyLink, for instance, follows a process where:

a. The app encrypts the SSID and password into a series of IP addresses.
b. The app transmits each IP address with a null character while simultaneously broadcasting the PT_SCAN message.
c. The smart device detects the traffic pattern, extracts the Wi-Fi credentials, and connects to the network.
d. The device then sends a PT_SCAN response to the app, which includes its MAC address and device key (EC public key).

7) Device Initialization

Once the app retrieves the MAC address, it sends a request to the cloud containing the MAC address, product_uuid, and user account details. The cloud verifies the ownership and responds with a message containing:

a. Feed_id and access_key
b. A locally generated encryption key (local_key)

The app then encrypts the feed_id and access_key before sending them to the device using a PT_WRITEACCESSKEY message. The device stores these credentials and sends a PT_AUTH request to the cloud to authenticate itself. The cloud responds by generating a session_key, encrypting it with the access_key, and sending it back in a PT_AUTH response. This ensures secure remote communication.

8) Communication Security

For smart home deployment, secure communication protocols are essential to protect data transmission. Various security techniques, such as KeyManagementSystems(KMS), ensure authentication and encryption of data exchanges. Implementing these protocols minimizes the risk of cyber threats and unauthorized access.

8.3. Secure Communication Protocols

Various wireless communication technologies are used in home automation to ensure seamless connectivity, efficient data transfer, and reliable performance. Each technology has distinct features, such as data rate, range, and power consumption. Below is an overview of the most commonly used wireless communication technologies in smart home applications.

1) Wi-Fi

Wi-Fi is the most widely used wireless communication technology in home automation. Based on the IEEE 802.11 standard, it operates on 2.4 GHz, 5 GHz, and 6 GHz frequency bands and supports data rates of up to 300 Mbps. Wi-Fi offers high-speed and secure communication with a range of up to 100 meters [24]. Further advancements, such as small cell technology, can enhance Wi-Fi networks by improving spectrum efficiency and communication reliability [25].

2) LTE (Long-Term Evolution)

LTE, originally developed for high-speed data transfer between mobile devices, is based on GSM/UMTS standards [26]. The enhanced version, LTE-A (LTE-Advanced), supports higher bandwidths of up to 100 MHz, offering improved coverage, higher throughput, and lower latency [25].

3) ZigBee

ZigBee is a low-power, wireless personal area network (WPAN) technology based on IEEE 802.15.4. It is widely used in home automation due to its low data rate (up to 250 kbps) and long battery life (up to 10 years). ZigBee operates on multiple frequency bands, primarily 2.4 GHz, and has a typical transmission range of up to 100 meters, depending on power output and environmental factors.

4) Z-Wave

Z-Wave is a low-power, cost-effective wireless communication technology designed for remote control applications. It supports data rates of up to 40 kbps and has a coverage range of up to 30 meters. Operating on the 2.4 GHz frequency

band, Z-Wave is commonly used in smart home security and automation.

5) Bluetooth & Bluetooth Low Energy (BLE)

Bluetooth is based on IEEE 802.15.1 and is widely used for short-range wireless communication. It operates on 2.4 GHz, supports data rates of up to 21 kbps, and has an operating range of up to 100 meters. Bluetooth is preferred for home automation due to its low power consumption, making it suitable for short-distance communication [27].

Bluetooth Low Energy (BLE) is a specialized version designed for low-power monitoring applications. Compared to classic Bluetooth, BLE consumes significantly less power and operates on the 2.4 GHz band, making it ideal for IoT applications [25].

6) EnOcean

EnOcean is an energy-harvesting wireless technology, meaning it generates power from natural sources such as ambient light. It is a cost-efficient solution for battery-less equipment and has extremely low maintenance costs. EnOcean operates on 902 MHz and 315 MHz, with a data rate of up to 125 kbps [24].

7) Wave2M

Wave2M is designed for ultra-low-powerlong-range transmission of small amounts of data. It can cover distances of upto1000meters, supports data rates of upto100kbps, and operates on the 2.4GHz frequency band [33].

8) RFID (Radio-Frequency Identification)

RFID is a bi-directionalradiofrequencyidentificationsystem that consists of tags and readers. It can be integrated with handheld computing devices or personal computers and can coexistwithtechnologiessuchasZigBeeandWi-Fi. RFID's detection range varies from 10cmto200meters, supporting data rates of upto4Mbps and operating across a wide frequency spectrum of 120kHzto10GHz [34].

9) ONE-NET

ONE-NET is an open-sourcestandardforlow-cost, low-powerwirelessnetworks. It is designed for applications such ashomeautomation, securitymonitoring, devicecontrol, andsensornetworks. ONE-NET supports a coverage area of upto100meters with data rates of upto38.4kbps, operating at 915MHz [35].

Table 5. *Comparison of wireless Technologies.*

Technology	Cost	Power	Speed	Operating Frequency	Operating Range (upto)
WIFI	High	High	300 Mbps	2.4GHz	100
ZigBee	Low	Low	250Kbps	2.4GHz	100
Z-Wave	Low	Low	30Kbps	2.4GHz	30
Bluetooth	Low	Low	21Kbps	2.4GHz	100
IEEE 802.15.3a	High	High	20Mbps-1.3Gbps	3.1-10GHz	10
EnOcean	Low	Moderate	125Kbps	315&902MHz	30
Wave2M	Low	High	100Kbps	2.4GHz	1000
RFID	Low	Low	4Mbps	120KHz-10GHz	10cm- 200m
ONE- NET	Low	Low	38.4Kbps	915 MHz	100
LTE	High	High	50-100Mbps	450-2600MHz	Mobile

9. Problems and Challenges

Interoperability:

Interoperability refers to the ability of systems, applications, and services to work together seamlessly and predictably. It is a critical concern in smart home ecosystems, as consumers demand devices that are easy to connect and use. However, smart home devices often come from various vendors with different network interfaces, making interoperability essential for achieving joint task execution. While many devices now operate on widely adopted protocols like Wi-Fi and Zigbee, which facilitate interoperability across a broad range of devices, challenges remain. Although industry standards have been established, there are still areas requiring improvement. For instance, in [28], the author highlights the ongoing issues related to interoperability and connectivity in smart home systems.

Self-Management:

Intelligent systems in smart homes must be capable of self-monitoring and notifying users of potential issues before they escalate into critical situations. A key requirement for sensor nodes is the ability to adapt to environmental changes autonomously, without human intervention. These systems

should also collaborate independently with other devices to ensure seamless operation. In [28], the author provides a detailed explanation of the self-management challenges faced by smart home systems, emphasizing the need for autonomy and adaptability.

Maintainability:

Maintainability is a crucial aspect of any smart home network, reflecting its reliability and durability over time. Networks must handle various changes, such as failing nodes, depleted batteries, and the introduction of new tasks. To address these challenges, the system should continuously monitor its performance and adjust operational parameters as needed. For example, it may need to prioritize energy efficiency by reducing data quality when resources are limited, as discussed in [28].

Bandwidth:

Bandwidth management is a significant challenge in IoT connectivity, especially as the number of connected devices continues to grow, generating massive amounts of data. Applications like video streaming, which demand high bandwidth, exacerbate this issue. To ensure smooth operation, smart home systems must be capable of transferring data efficiently, without delays or loss. This requires robust network design and optimization, as highlighted in [28].

Power Consumption:

Power consumption is a critical concern for IoT devices in smart homes. These devices constantly send and receive signals, and their CPUs process data, leading to significant energy use. An efficient IoT network must minimize energy consumption while maintaining high performance. However, there is a trade-off between power usage and data transmission: systems that send and receive more data will inherently consume more power. Striking the right balance is essential, as noted in [28].

Integration:

As the smart home industry grows, numerous companies are producing a wide variety of smart devices for homes and cities. While this provides consumers with a wealth of options, it also introduces integration challenges. Devices from different brands often operate on different frequencies or protocols, leading to compatibility issues and increased complexity. Addressing these integration problems is vital for creating a cohesive and user-friendly smart home ecosystem [36].

Data Storage:

The rapid growth of IoT applications has led to an exponential increase in data collection. Storing this vast amount of data requires significant storage capacity, which can drive up costs. Efficient data management strategies, such as cloud storage and edge computing, are essential to mitigate these challenges and ensure scalability [38].

High Cost of Ownership:

The adoption of smart home technology often involves significant upfront costs. Consumers need to purchase a variety of devices, including sensors, relays, smart appliances, and embedded systems. While these devices offer advanced functionality, their high cost can be a barrier to widespread adoption. The industry continues to face challenges in producing and installing smart equipment at affordable prices, making cost reduction a key area for innovation.

By addressing these challenges—interoperability, self-management, maintainability, bandwidth, power consumption, integration, data storage, and cost—smart home systems can become more efficient, reliable, and accessible to a broader audience [39].

9.1. Open Research Issues

Smart homes have garnered significant attention in recent years, with many challenges and issues being identified. While substantial progress has been made, several areas still require improvement. Some issues are critical, while others have been somewhat addressed but still demand further exploration. Below are some open research issues that need more focused attention:

1) *Transformation of Conventional Homes to Smart Homes:* A major challenge lies in converting traditional homes into smart homes with minimal cost and design alterations. Upgrading a house to a smart home often requires extensive modifications, from sensors to appliances. Smart appliances tend to be costly, which makes them unaffordable for many consumers. Current research lacks reasonable solutions to this problem, with many suggesting that smart homes should be built from scratch due to the substantial physical changes involved [60].
2) *Interoperability Between Different Brands:* Different manufacturers create smart devices based on varying standards, leading to significant interoperability issues. Although some global standards have been developed, the problem persists, especially when consumers purchase products from different manufacturers. These inconsistencies result in integration difficulties and operational issues across diverse devices, undermining the seamless functioning of smart homes [61].
3) *Inflexibility of Systems:*Many smart home systems come with pre-configured functionalities that may not fully align with users' individual preferences and evolving needs. Research indicates that consumers increasingly seek greater customization and control over their smart home applications. For example, within a household, different family members may want to personalize their entertainment experience, such as watching different TV shows simultaneously on multiple screens. However, rigid system architectures and limited adaptability make it difficult to accommodate such personalized experiences. Addressing this challenge requires more modular, user-configurable automation frameworks that allow seamless integration of customized preferences, AI-driven adaptive settings, and cross-device interoperability. Enhancing system flexibility is key to driving

broader adoption and long-term user satisfaction in smart home automation [62].

4) *Energy Efficiency:* Energy consumption remains a significant concern in smart homes, particularly regarding communication devices. The energy usage of various devices is directly tied to their performance, and while multiple communication protocols like ZigBee, Wi-Fi, and Bluetooth exist, each has its own advantages and limitations. This area requires more focused research to optimize energy efficiency and balance performance across different devices and protocols [63].
5) *Security Challenges:* As wireless technology continues to evolve, the security challenges associated with smart homes also grow. While there has been significant progress, current security measures remain insufficient. Key security concerns include authentication, denial-of-service (DoS) attacks, data breaches, and identity theft. More robust solutions are required to ensure the safety and privacy of users within smart homes [64].

9.2. Potential Solutions

1) *Transforming Conventional Homes into Smart Homes:* Upgrading traditional homes to smart homes should not be an expensive or complex endeavor. One possible approach is to develop retrofit solutions such as smart plugs, modular sensors, and AI-driven hubs that seamlessly integrate with existing electrical systems and appliances. Additionally, the focus should shift toward affordable smart devices, ensuring that cost-effective, energy-efficient alternatives become widely available. Another promising avenue is cloud-based integration, which allows older appliances to gain smart functionalities through software enhancements rather than costly hardware replacements.
2) *Enhancing Interoperability Between Different Brands*: The lack of standardized communication between devices from different manufacturers remains a significant barrier to seamless smart home automation. A viable solution is to promote universal communication standards, such as Matter, which facilitate interoperability across various brands. Additionally, AI-powered translators can act as intermediaries, enabling devices that operate on different protocols to communicate effectively. Further, industry-wide standardization initiatives should be encouraged to push manufacturers toward greater compatibility, ensuring a more user-friendly and cohesive smart home ecosystem.
3) *Increasing System Flexibility:* Many smart home systems are pre-configured with limited customization options, which can restrict their usability for diverse households. To address this, modular automation platforms should be developed, allowing users to tailor automation settings based on their preferences. Furthermore, AI-driven adaptation can be employed to enable smart systems to learn from user behavior and dynamically adjust their settings. Another potential improvement is the introduction of personalized control interfaces, where voice assistants and mobile applications allow different household members to customize their experience according to their specific needs.
4) *Optimizing Energy Efficiency:* Despite the promise of energy savings, the growing number of connected devices in smart homes has led to increased energy consumption. A practical solution is to introduce energy-aware scheduling, which optimizes the usage of smart devices by aligning their operation with real-time energy demand and pricing. Additionally, expanding the use of low-power communication protocols such as ZigBee, Thread, and LoRaWAN can help reduce the energy footprint of always-on devices. Another effective strategy is to develop self-sustaining devices that leverage renewable energy sources like solar panels and kinetic energy harvesting to function independently of the main power grid.
5) *Strengthening Smart Home Security*: As smart homes become more interconnected, they also become more vulnerable to cyber threats. To mitigate these risks, implementing end-to-end encryption for all communications between smart devices can significantly enhance data security. Additionally, AI-powered intrusion detection systems can continuously monitor network activity and detect potential security breaches in real time. Another promising approach is the adoption of decentralized security frameworks, such as blockchain-based authentication systems, which distribute security verification across multiple nodes, reducing the risk of a single point of failure.

By addressing these challenges through innovative and practical solutions, smart homes can become more accessible, efficient, and secure, ultimately fostering greater adoption and long-term sustainability.

10. Conclusion

Smart homes are revolutionizing the way we live, bringing automation, security, and efficiency to modern urban spaces. As part of the broader vision of smart cities, these interconnected systems use IoT technologies to enhance daily life whether it's controlling lighting, monitoring energy consumption, or securing homes with advanced biometric authentication. While the benefits of smart homes are undeniable, their widespread adoption faces several challenges, including security vulnerabilities, interoperability issues, and high implementation costs. This paper explored the technological advancements in smart home automation, covering key applications, core components, and the evolving security landscape to ensure these systems remain safe and reliable.

Despite remarkable progress, there are still open questions about how to integrate diverse devices seamlessly, strengthen

data protection, and make smart home solutions more affordable and accessible. As technology continues to evolve, researchers and industry experts must address these challenges to create truly intelligent, secure, and adaptable living environments. The future of smart homes is promising, but its success hinges on balancing convenience with security and efficiency. By tackling these issues head-on, we can ensure that smart homes not only enhance urban living but also offer a safe, sustainable, and interconnected future for all.

Abbreviations

BLE	Bluetooth Low Energy
DDoS	Distributed Denial of Service
DNS	Domain Name System
GSM	Global System for Mobile Communications
IoT	Internet of Things
LAN	Local Area Network
LTE	Long-Term Evolution
MAC	Message Authentication Codes
MAN	Metropolitan Area Network
PDoS	Permanent Denial of Service
RFID	Radio-Frequency Identification
SIG	Special Interest Group
UMTS	Universal Mobile Telecommunications System
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WPAN	Wireless Personal Area Network
ZTA	Zero Trust Architecture

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] A. Alkandari, A. Alhammadi, and A. Alghamdi, "Smart Cities: Survey," Journal of Advanced Computer Science and Technology Research Vol. 2 No. 2, June 2012, 79-90.

[2] Hall, Robert E., B. Bowerman, Joseph Braverman, J. Taylor, Helen Todosow, and U. Von Wimmersperg. *The vision of a smart city*. No. BNL-67902; 04042. Brookhaven National Lab.(BNL), Upton, NY (United States), 2000.

[3] S. Ijaz, H. Zubair, and A. U. Rehman, "Smart Cities: A Survey on Security Concerns," *International Journal of Advanced Computer Science and Applications*, vol. 7, 2016. https://doi.org/10.14569/IJACSA.2016.070277

[4] A. J. Bernheim Brush, Bongshin Lee, RatulMahajan, SharadAgarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11). Association for Computing Machinery, New York, NY, USA, 2115-2124. https://doi.org/10.1145/1978942.1979249

[5] Dahmen, J., Cook, D. J., Wang, X., & Honglei, W. (2017). Smart Secure Homes: A Survey of Smart Home Technologies that Sense, Assess, and Respond to Security Threats. *Journal of reliable intelligent environments*, *3*(2), 83-98. https://doi.org/10.1007/s40860-017-0035-0

[6] Alshamsi, O., Shaalan, K., & Butt, U. (2024). Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach. *Information*, *15*(10), 631. https://doi.org/10.3390/info15100631

[7] S. M. Shaheed, M. S. B. Ilyas, J. A. Sheikh and J. Ahamed, "Effective smart home system based on flexible cost in Pakistan," *2017 Fourth HCT Information Technology Trends (ITT)*, Al Ain, United Arab Emirates, 2017, pp. 35-38, https://doi.org/10.1109/CTIT.2017.8259563

[8] P. Waghmare, P. Chaure, M. Chandgude and A. Chaudhari, "Survey on: Home automation systems," *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, Tirunelveli, India, 2017, pp. 7-10, https://doi.org/10.1109/ICOEI.2017.8300864

[9] P. P. Gaikwad, J. P. Gabhane and S. S. Golait, "A survey based on Smart Homes system using Internet-of-Things," *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, Melmaruvathur, India, 2015, pp. 0330-0335, https://doi.org/10.1109/ICCPEIC.2015.7259486

[10] V. Yadav, S. Borate, S. Devar, R. Gaikwad and A. B. Gavali, "Smart home automation using virtue of IoT," *2017 2nd International Conference for Convergence in Technology (I2CT)*, Mumbai, India, 2017, pp. 313-317, https://doi.org/10.1109/I2CT.2017.8226143

[11] M. Asadullah and A. Raza, "An overview of home automation systems," *2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI)*, Rawalpindi, Pakistan, 2016, pp. 27-31, https://doi.org/10.1109/ICRAI.2016.7791223

[12] N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014, https://doi.org/10.1109/COMST.2014.2320093

[13] C. -L. Hu *et al*., "IoT-based LED lighting control in smart home," *2018 IEEE International Conference on Applied System Invention (ICASI)*, Chiba, Japan, 2018, pp. 877-880, https://doi.org/10.1109/ICASI.2018.8394405

[14] J. Margulies, "Garage Door Openers: An Internet of Things Case Study," in *IEEE Security & Privacy*, vol. 13, no. 4, pp. 80-83, July-Aug. 2015, https://doi.org/10.1109/MSP.2015.80

[15] T. Balikhina, A. A. Maqousi, A. AlBanna and F. Shhadeh, "System architecture for smart home meter," *2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS)*, Amman, Jordan, 2017, pp. 1-5, https://doi.org/10.1109/IT-DREPS.2017.8277811

[16] "Applications of Smart Homes," *Link Labs*, 17 Mar. 2015. [Online]. Available: https://www.link-labs.com/blog/applications-of-home-automation [Accessed: 16 Dec. 2024].

[17] K. Bing, L. Fu, Y. Zhuo and L. Yanlei, "Design of an Internet of Things-based smart home system," *2011 2nd International Conference on Intelligent Control and Information Processing*, Harbin, China, 2011, pp. 921-924, https://doi.org/10.1109/ICICIP.2011.6008384

[18] N. Jose, M. S. R. M., "The Best Home Automation Apps to Make Your Life Easier," [Online]. Available: https://www.thinklions.com/blog/best-home-automation-apps/#6_Samsung_SmartThings_A_Central_Hub_For_Home_Automation [Accessed: 4 Dec. 2024].

[19] H. AlShu'eili, G. S. Gupta and S. Mukhopadhyay, "Voice recognition based wireless home automation system," *2011 4th International Conference on Mechatronics (ICOM)*, Kuala Lumpur, Malaysia, 2011, pp. 1-6, https://doi.org/10.1109/ICOM.2011.5937116

[20] S. Sen, A. K. M. F., "Design of an Intelligent Voice Controlled Home Automation System," *International Journal of Computer Applications*, vol. 121, pp. 39-42, 2015, https://doi.org/10.5120/21619-4904

[21] R. Piyare, K. K. D., "Internet of Things: Ubiquitous Home Control and Monitoring System Using Android-based Smartphone," *International Journal of Internet of Things*, vol. 2, pp. 5-11, 2013, https://doi.org/10.5923/j.ijit.20130201.02

[22] Khader, R., & Eleyan, D. (2021). Survey of DoS/DDoS attacks in IoT. *Sustainable Engineering and Innovation*, *3*(1), 23-28. https://doi.org/10.37868/sei.v3i1.124

[23] Abaimov, S. (2024). Understanding and Classifying Permanent Denial-of-Service Attacks. *Journal of Cybersecurity and Privacy*, *4*(2), 324-339. https://doi.org/10.3390/jcp4020016

[24] M. Kuzlu, M. Pipattanasomporn and S. Rahman, "Review of communication technologies for smart homes/building applications," *2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, Bangkok, Thailand, 2015, pp. 1-6, https://doi.org/10.1109/ISGT-Asia.2015.7437036

[25] F. Al-Turjman, E. Ever and H. Zahmatkesh, "Small Cells in the Forthcoming 5G/IoT: Traffic Modelling and Deployment Overview," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 28-65, Firstquarter 2019, https://doi.org/10.1109/COMST.2018.2864779

[26] G. V. Crosby and F. Vafa, "Wireless sensor networks and LTE-A network convergence," *38th Annual IEEE Conference on Local Computer Networks*, Sydney, NSW, Australia, 2013, pp. 731-734, https://doi.org/10.1109/LCN.2013.6761322

[27] P. McDermott-Wells, J. W. F., "What is Bluetooth?," *IEEE Potential*, vol. 23, pp. 33-35, 2004.

[28] S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, Muscat, Oman, 2016, pp. 1-4, https://doi.org/10.1109/ICBDSC.2016.7460395

[29] "Authentication Hacking: What are Authentication Hacking Attacks?" *Acunetix*, [Online]. Available: https://www.acunetix.com/websitesecurity/authentication/ [Accessed: 21 Dec. 2024].

[30] B. O'Shea, T. P. F., "How to Prevent Identity Theft," *Nerd-Wallet*, 4 Oct. 2018. [Online]. Available: https://www.nerdwallet.com/blog/finance/how-to-prevent-identity-theft/ [Accessed: 20 Dec. 2024].

[31] "Here is How to Fend Off a Hijacking of Home Devices," [Online]. Available: https://www.nytimes.com/2017/02/01/technology/personaltech/stop-hijacking-home-devices.html [Accessed: 20 Dec. 2024].

[32] Briland, M., & Bouquet, F. (2021). A language for modelling false data injection attacks in Internet of Things. *2021 IEEE/ACM 3rd International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT)*, 1-8. https://doi.org/10.1109/SERP4IoT52556.2021.00007

[33] Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). *Low Power Wide Area Networks: An overview*. *IEEE Communications Surveys & Tutorials*, *19*(2), 855-873. https://doi.org/10.1109/COMST.2017.2652320

[34] Batyha, R. M., Boddepalli, E., Deepika, N. M., Swathi, B., Kumar, M., & Kiranmayee, P. (2025). RFID-based Internet of Things Services and Infrastructures for Smart Homes. In *Recent Trends In Engineering and Science for Resource Optimization and Sustainable Development* (pp. 202-205). CRC Press.

[35] Shan, Y., Su, Y., Lin, J., & Shan, T. (2024). IoT Communication Based on MQTT and OneNET Cloud Platform in Big Data Environment. Preprints. https://doi.org/10.20944/preprints202401.1250.v1

[36] Madadi-Barough, S., Ruiz-Blanco, P., Lin, J., Vidal, R., & Gomez, C. (2024). *Matter: IoT interoperability for smart homes*. arXiv. https://arxiv.org/abs/2405.01618

[37] VinodVeeramachaneni. (2024). Emerging Authentication Technologies for Zero Trust in IoT Systems. Journal of Advance Research in Mobile Computing, 7(1), 7-21. https://doi.org/10.5281/zenodo.14166892

[38] Monga, S. K., R, S. K., & Simmhan, Y. (2019). *ElfStore: A resilient data storage service for federated edge and fog resources*. *arXiv*. https://doi.org/10.48550/arXiv.1905.08932

[39] Gayo-Abeleira, M., Rodr ́guez, F. J., Santos, C., Wu, Y., Wu, Y., Vasquez, J. C., & Guerrero, J. M. (2023). *Design and implementation of multiprotocol framework for residential prosumer incorporation in flexibility markets*. *Internet of Things*, *23*, 100897. https://doi.org/10.1016/j.iot.2023.100897

[40] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, USA, 2017, pp. 618-623, https://doi.org/10.1109/PERCOMW.2017.7917634

[41] R. R., S. N., "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 2013, pp. 2266-2279, 2013, https://doi.org/10.1016/j.comnet.2012.12.018

[42] Gaboardi, Marco, and Chris J. Skinner. "Special issue on the theory and practice of differential privacy." *Journal of Privacy and Confidentiality* 7, no. 2, 2017, https://doi.org/10.29012/jpc.v7i2.647

[43] H. Zheng, H. Zhang and L. Pan, "Modeling and Analysis of ZigBee Based Smart Home System," *2014 5th International Conference on Digital Home*, Guangzhou, China, 2014, pp. 242-245, https://doi.org/10.1109/ICDH.2014.53

[44] Islam, N., Zia, M. F., & Syed, D. (2023). An Overview of Security Issues in Cognitive Radio Ad Hoc Networks. In M. Habib (Ed.), *Perspectives and Considerations on the Evolution of Smart Systems* (pp. 213-246). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-6684-7684-0.ch009

[45] M. F. Zia, "Secrecy and Resilience in Next-Gen Wi-Fi: Exploring a Multi-User Down-Link Non-Orthogonal Transmission Framework," 2024 Intermountain Engineering, Technology and Computing (IETC), Logan, UT, USA, 2024, pp. 1-6, https://doi.org/10.1109/IETC61393.2024.10564473

[46] Zia, M. F., Furqan, H. M., & Hamamreh, J. M. (2021). Multi-cell, Multi-user, and Multi-carrier Secure Communication Using Non-Orthogonal Signals' Superposition with Dual-Transmission for IoT in 6G and Beyond. *RS Open Journal on Innovative Communication Technologies*, *2*(3). https://doi.org/10.46470/03d8ffbd.08b7bd1d

[47] Zia, M. F., & Hamamreh, J. M. (2020). An Advanced Non-Orthogonal Multiple Access Security Technique for Future Wireless Communication Networks. *RS Open Journal on Innovative Communication Technologies*, *1*(2). https://doi.org/10.46470/03d8ffbd.19888ce7

[48] Zia, M. F., & Hamamreh, J. M. (2020, September). An advanced noma security technique for future wireless communication. In *Workshop on Information and Communications Technologies, International Conference on Software, Telecommunications and Computer Networks (SoftCOM)* (pp. 38-43).

[49] Shalan, M., Hasan, M. R., Bai, Y., & Li, J. (2025). Enhancing Smart Home Security: Blockchain-Enabled Federated Learning with Knowledge Distillation for Intrusion Detection. Smart Cities, 8(1), 35. https://doi.org/10.3390/smartcities8010035

[50] Sharma, A., & Babbar, H. (2023). Machine learning-based anomaly detection in the Internet of Things. 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), 1-6. https://doi.org/10.1109/ASIANCON58793.2023.10270100

[51] Bajwa, N. T., Anjum, A., & Khan, M. A. (2023). A blockchain-based lightweight secure authentication and trust assessment framework for IoT devices in fog computing. 2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET), 30-35. https://doi.org/10.1109/HONET59747.2023.10374800

[52] Wang, Q., Dai, H.-N., Li, X., Shukla, M. K., & Imran, M. (2020). Artificial noise aided scheme to secure UAV-assisted Internet of Things with wireless power transfer. Computer Communications, 164, 1-12. https://doi.org/10.1016/j.comcom.2020.09.017

[53] Endler, M., Silva, A., & Cruz, R. A. M. S. (2017). An approach for secure edge computing in the Internet of Things. 2017 1st Cyber Security in Networking Conference (CSNet), 1-8. https://doi.org/10.1109/CSNET.2017.8241993

[54] Chahal, R. K., Kumar, N., & Batra, S. (2020). Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Computer Communications*, *150*, 13-46.

[55] Wang, R., & Yan, Y. (2022). A survey of secure boot schemes for embedded devices. 2022 24th International Conference on Advanced Communication Technology (ICACT), 224-227. https://doi.org/10.23919/ICACT53585.2022.9728840

[56] Ma, Q., Tan, H., & Zhou, T. (2023). Mutual authentication scheme for smart devices in IoT-enabled smart home systems. Computer Standards & Interfaces, 86, 103743. https://doi.org/10.1016/j.csi.2023.103743

[57] Lin, S., Cui, L., & Ke, N. (2024). End-to-End Encrypted Message Distribution System for the Internet of Things Based on Conditional Proxy Re-Encryption. Sensors, 24(2), 438. https://doi.org/10.3390/s24020438

[58] Song, Mei. (2024). Role of Continuous Monitoring and Threat Detection in Zero Trust RPA Environments.

[59] Yousefnezhad, N., Malhi, A., & Främling, K. (2020). Security in product lifecycle of IoT devices: A survey. Journal of Network and Computer Applications, 171, 102779. https://doi.org/10.1016/j.jnca.2020.102779

[60] Shakeri, M., & Amin, N. (2018). Transformation of Conventional Houses to Smart Homes by Adopting Demand Response Program in Smart Grid. InTech. https://doi.org/10.5772/intechopen.74780

[61] Bakshi, P., & Kumar, S. R. (2024). Interoperability and open standards for home connected devices: Unlocking benefits for the power sector.

[62] Parag, Y., & Butbul, G. (2018). Flexiwatts and seamless technology: Public perceptions of demand flexibility through smart home technology. *Energy Research & Social Science*, *39*, 177-191.

[63] Prieto González, L., Fensel, A., Gómez Berbís, J. M., Popa, A., & de Amescua Seco, A. (2021). A survey on energy efficiency in smart homes and smart grids. *Energies*, *14*(21), 7273.

[64] Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. *Electronics*, *13*(16), 3343.