# A Survey on Secure Smart Homes in the Age of IoT-Enabled Smart Cities

Muhammad Furqan Zia[1], Maria Siddiqua[2], Fadi Al Turjman[3]
[1]Department of Electrical and Computer Engineering, University of Quebec at Trois-Rivieres, QC, Canada
[2]Department of Artificial Intelligence and Data Science, The National University of Computer and Emerging, Sciences (FAST-NUCES), Karachi, Pakistan
[3]Department of Information Systems, AI and Robotics Institute, Near East University, Nicosia, Türkiye

Muhammad.Furqan.Zia@uqtr.ca, Maria.Siddiqua@nu.edu.pk, Fadi.alturjman@neu.edu.tr

**Abstract—** The rapid growth of urban areas and advancements in information technology have paved the way for the development of smart cities and homes, leveraging the Internet of Things (IoT). Smart cities and homes represent the future of urban living, offering enhanced efficiency, convenience, and sustainability. This survey paper provides a comprehensive overview of the progress made in the domain of smart homes, focusing on the integration of IoT technologies. It explores the architectures, applications, devices, and communication technologies that have been implemented to achieve desired outcomes in smart home environments. Additionally, the paper highlights the key challenges researchers are addressing, particularly in the realm of security, to ensure the safe and reliable operation of smart homes within smart cities. By examining the current state of the art, this paper aims to provide insights into the future direction of secure smart homes and their role in the broader ecosystem of smart cities.

**IndexTerms—**Smart city, IoT security, Home Automation, Communication technologies, IoT challenges, Secure Smart homes.

## I. 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 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 human intervention. 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. This survey 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 II discusses the background, objectives, and constraints of smart homes in smart cities. Section III 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 IV and V. Section VI categorizes the devices used in smart homes, while Section VII and VIII explain secure deployment strategies and wireless communication protocols, respectively. Section IX addresses critical challenges such as security and privacy, along with potential countermeasures. Section X provides insights into the deployment of smart homes, and Section XI identifies open research issues to guide future studies. Finally, Section XII concludes the paper by summarizing the key findings and their implications for the future of smart homes in smart cities.

To assist readers, a list of abbreviations and their definitions is provided in Table I. 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.

*Table 1 Table of Abbreviations*

| **Term** | **Abbreviation** |
|---|---|
| IoT | Internet of things |
| LAN | Local Area Network |
| WAN | Wide Area Network |
| MAN | Metropolitan Area Network |
| RFID | Radio-frequency identification |
| WPAN | Wireless Personal Area Network |
| DDoS | Distributed Denial of Service |
| PDoS | Permanent Denial of Service |
| Wi-Fi | Wireless Fidelity |
| GSM | Global System for Mobile Communications |
| BLE | Bluetooth Low Energy |
| SIG | Special Interest Group |
| LTE | Long-Term Evolution |
| UMTS | Universal Mobile Telecommunications System |
| DNS | Domain Name System |

## II. BACKGROUND

As urban populations continue to grow, cities face significant challenges in resource management, infrastructure sustainability, 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. 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:

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

- **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.

- **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.
- **Security Concerns**: Research in [9] discusses issues related to controlling multiple devices simultaneously, ensuring data security, and addressing integration challenges within smart homes.
- **Communication Efficiency**: In [11], various communication techniques were evaluated based on cost, efficiency, and data transmission rates.
- **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.

## III. APPLICATIONS

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:

- **Base Station**: Includes components like IoT gateways, appliance trackers, and data repositories.
- **Appliance Controller**: Equipped with sensors and relay modules to manage connected devices.
- **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.

### 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:

- **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.
- **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. Reference [16] highlights 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:

- **CCTV Cameras**: Provide real-time surveillance and recording.
- **Motion Sensors**: Detect unauthorized movement and trigger alarms.
- **Biometric Devices**: Enable secure access through fingerprint or facial recognition.
- **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:

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

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

## IV. 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.

**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.

**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.

**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 smartphones 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.

## V. TRUSTWORTHY COMPUTING MODELS

Several trustworthy computing models have been developed for smart homes, each offering unique advantages and features. Different modeling techniques include feature modeling and variability modeling. In [37], the author introduced an object-based IoT management model, while in [38], a ZigBee-based smart home system was analyzed. Based on the literature, many researchers favor feature modeling due to its robust support for variability reasoning and system functionality enhancement.

In [39], the author explored feature modeling in the context of smart homes, illustrating how features are organized in a hierarchical tree structure with variability relationships such as optional, mandatory, single-choice, and multiple-choice options. The figure below represents a smart home feature model, incorporating automated illumination, multimedia systems, garage management, and security functionalities. The blue boxes highlight active features, whereas black boxes indicate potential future variations.

### *A. TECHNIQUES 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:

1. **Voice Recognition-Based Home Automation**
2. **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 the Arduino and the smartphone is 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:

1. **Home Environment:** Contains hardware interface modules and a home gateway to manage smart devices.
2. **Home Gateway:** Acts as a bridge between the home environment and external networks.
3. **Remote Environment:** Enables authorized users to monitor and control home appliances remotely via smartphones using Wi-Fi, 3G, or 4G networks.

*Table3. Comparison between Home Automation control Techniques*

| Technology | Cost | Efficiency | Flexibility | Response |
|---|---|---|---|---|
| **Voice Recognition** | Moderate | Moderate | High | Moderate |
| **IoT Based** | High | High | High | High |

## VI. 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:

- **Fire Sensors:** Detect smoke or fire and activate water sprinklers for fire suppression.
- **Moisture Sensors:** Identify moisture levels in walls, helping to prevent water damage and mold growth.
- **Motion Detectors:** Detect movement within the home and can trigger lighting or security alerts.
- **Light Sensors:** Measure ambient light levels and automatically turn lights on or off as needed.
- **Water Sensors:** Monitor water levels in tanks and help prevent overflow or shortages.
- **Pressure Sensors:** Detect pressure variations inside and outside the home, providing valuable data for home automation systems.
- **Gas Sensors:** Identify the presence of harmful gases, such as carbon monoxide or natural gas leaks, and trigger alerts for safety.
- **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:

- **Kitchen Appliances:** Refrigerators, kettles, juicers, microwaves, blenders, and cookers.
- **Washroom Appliances:** Washing machines, hand dryers, and toilet roll dispensers.
- **Living Room Appliances:** Air conditioners, fans, lights, and heaters.

**3. Entertainment Devices**

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

- **Home Theater Systems:** Smart TVs, DVD players, and high-quality speakers.
- **Gaming Devices:** Computers, monitors, gaming consoles such as Xbox and PlayStation.
- **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:

- **CCTV Cameras:** Provide real-time surveillance and remote monitoring.
- **Alarms:** Trigger alerts in case of unauthorized access or emergencies.
- **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 4. 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). **LivingRoom:**(AirConditioners, Fans,Lights,Heaters). |
| **Entertainment Devices** | **HomeTheaterDevices:**(TVs,DVD Box, Speakers). **Gaming Devices:** (Computers, Monitors, Xbox, PlayStation). **Music devices:** (Speakers, Microphones). |
| **SecurityDevices** | CCTV Cameras, Alarms and monitoringscreens |

## VII. 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 vulnerable to attacks.

**2. Secure Connection Applications**

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

- The developer or company behind the application.
- The app’s security rating and reviews.
- 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:

- Scanning the QR code on the device or selecting the correct product title from the app.
- The app retrieving a product_uuid and sending it to the cloud.
- The app broadcasting a PT_SCAN message containing the product_uuid and the application's EC public key.
- 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:

- The app encrypts the SSID and password into a series of IP addresses.
- The app transmits each IP address with a null character while simultaneously broadcasting the PT_SCAN message.
- The smart device detects the traffic pattern, extracts the Wi-Fi credentials, and connects to the network.
- 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:

- feed_id and access_key
- 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 Key Management Systems (KMS), ensure authentication and encryption of data exchanges. Implementing these protocols minimizes the risk of cyber threats and unauthorized access.

## VIII. 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, 3.5 GHz, and 5 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-power long-range transmission of small amounts of data. It can cover distances of up to 1000 meters, supports data rates of up to 100 kbps, and operates on the 2.4 GHz frequency band.
**8. RFID (Radio-Frequency Identification)**
RFID is a bi-directional radio frequency identification system that consists of tags and readers. It can be integrated with handheld computing devices or personal computers and can coexist with technologies such as ZigBee and Wi-Fi. RFID's detection range varies from 10 cm to 200 meters, supporting data rates of up to 4 Mbps and operating across a wide frequency spectrum of 120 kHz to 10 GHz.
**9. ONE-NET**
ONE-NET is an open-source standard for low-cost, low-power wireless networks. It is designed for applications such as home automation, security monitoring, device control, and sensor networks. ONE-NET supports a coverage area of up to 100 meters with data rates of up to 38.4 kbps, operating at 915 MHz.

*Table5. Comparison of wirelessTechnologies*

| 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 | 3.1-10 GHz | 10 |
| **EnOcean** | Low | Moderate | 125Kbps | 315&902 MHz | 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 | 50-100 Mbps | 450-2600 MHz | Mobile |

## IX. 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 [29], 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 [29].
**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 [29].
**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 [29].
**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.
**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.
**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.

## X. SECURITYAND PRIVACY REQUIREMENTS FOR SMART HOME SERVICES

Secure smart homes are a critical necessity in today’s world. While these homes offer a variety of features, security remains the foremost concern for residents. To safeguard these homes, there are several essential requirements for security services. Numerous studies have explored the various security needs of smart homes. In [40], the author identifies some fundamental security and privacy requirements, including Data Confidentiality, Data Integrity, and Device-to-Device Authentication, among others. Additionally, security and privacy can be divided into several core categories such as confidentiality, integrity, and availability. By addressing and fulfilling these requirements, we can achieve a moderate level of security for smart homes. The following table outlines some of the key security requirements.

*Table6: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 [41][42]. |
| **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 [44]. 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 [43]. |
| **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 [46]. |

**Security Challenges:**

- **Authentication**: Authentication is the process of verifying the identity of communicating parties or users, ensuring that they are who they claim to be and that data is sent to the correct recipient. It is a fundamental aspect of security. Servers containing sensitive user information should grant access only to authenticated users. Solutions to combat these attacks include the use of strong passwords and the generation of random captchas [30].
- **Man-in-the-Middle Attacks**: This occurs when an attacker intercepts or manipulates communication between two systems. For example, an attacker could fake temperature data from a sensor and send it to a server or cloud. To prevent such attacks, employing strong cryptographic methods, secure authentication, and data integrity checks are essential.
- **Data and Identity Theft**: Data generated by insecure or poorly protected devices, such as wearables and home appliances, can be exploited by cybercriminals. Personal information can be stolen for fraudulent transactions and identity theft. Preventive measures include strengthening passwords, limiting the sharing of personal information,

and protecting mobile devices with strong passwords [31].

- **Masquerading**: In masquerading attacks, an entity masks its identity and impersonates another system or device using false identities, such as public keys. This technique is often used in conjunction with other attack methods. Prevention can be achieved by implementing a multi-step approval process and identity verification.
- **Eavesdropping**: Eavesdropping is a passive attack where an unauthorized third party intercepts ongoing communication without the consent of the communicating parties. This can include phone calls, instant messages, or other forms of internet-based communication. Encryption is the most effective solution to prevent this type of attack.
- **Device Hijacking**: In device hijacking, a hacker takes control of a smart device and uses it for malicious purposes. These attacks are difficult to detect because the basic functionality of the device remains unchanged, making it hard for users to notice. A single compromised device can infect other devices within the home. For instance, an attacker who compromises a thermostat may gain access to locks or other appliances, even changing PINs to restrict access for authorized users. To prevent device hijacking, it is crucial to strengthen passwords and regularly update device software [32].
- **Distributed Denial of Service (DDoS)**: A denial of service (DoS) attack occurs when an attacker renders a device or network resource temporarily unavailable to authenticated users. In DDoS attacks, multiple sources are involved, making it difficult to stop the attack by blocking a single source. For example, a compromised smart sensor could infect devices running the same software. To prevent these attacks, it is essential to deploy anti-DDoS hardware and software modules and protect DNS servers.
- **Permanent Denial of Service (PDoS)**: In PDoS, the damage caused by the attack is so severe that it permanently damages the device, necessitating its replacement or reinstallation. For example, BrickerBot exploits hard-coded passwords in IoT devices to cause permanent denial of service. Solutions to mitigate these risks include protecting DNS servers and strengthening firewall security.
- **False Information**: Attackers may transmit erroneous or manipulated information within the network, which can negatively impact the behavior of other devices or systems. This can be either intentional or unintentional, leading to misinformed actions or decisions.

**Security Countermeasures:**
To secure connected smart home devices, a comprehensive IoT security solution (device-to-cloud) should be implemented. This solution should not disrupt a service provider's or OEM's profitability or time-to-market. A comprehensive security solution should incorporate the following capabilities [47] [48]:

- **Secure Boot**: Secure boot uses cryptographic code-signing techniques to ensure that devices only run code generated by the device's OEM or another trusted party. With secure boot, hackers cannot replace the device's firmware with malicious code, helping to maintain the device's integrity.
- **Mutual Authentication**: When a smart home device connects to the network, it should undergo authentication before transmitting or receiving data. This ensures that the data originates from a legitimate device and source. Various cryptographic algorithms, such as Secure Hash Algorithm (SHA) and Digital Signature Algorithm (DSA), can be used for two-way authentication.
- **Secure Communication (Encryption)**: Encrypting data in transit between devices and their service infrastructure (such as the cloud) ensures that only authenticated users with the secret decryption key can access the data. For example, a smart thermostat that sends data to the operator must ensure the transmitted information remains protected and inaccessible to unauthorized parties.
- **Security Monitoring and Analysis**: This involves capturing data from across the system, including endpoint devices and network traffic, to identify potential security violations. Once threats are detected, a range of security actions is triggered according to the overall system's security policy. Monitoring can be done in real-time or post-event, enabling the detection of multiple potential attack patterns. It is critical to secure endpoint devices from tampering and data manipulation.
- **Security Lifecycle Management**: Lifecycle management enables service providers and OEMs to control the security of devices while they are operational. In the event of a cyber disaster, rapid over-the-air (OTA) device key replacement ensures minimal service disruption. Additionally, secure decommissioning of devices ensures that discarded devices cannot be repurposed or exploited to access services without authorization.

## XI. 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 [49][50]:

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.

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.

3. **Inflexibility of Systems**: Many smart home systems and equipment come with pre-installed functionalities that may not meet users' specific needs. Research shows that consumers often want more flexibility and personal control over applications. For instance, in a family, each person might want to watch their favorite TV show simultaneously. Structural changes to enable greater flexibility remain a significant barrier to the widespread adoption of home automation.

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 [51].

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 [52].

## XII. 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.

## References


1. Alkandari, A. Alhammadi, and A. Alghamdi, "Smart Cities: Survey," *Journal of Advanced Computer Science and Technology Research*, pp. 79-90, 2012.
2. J. Bowerman, L. Smith, and A. Williams, "The Vision of a Smart City," 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.
4. Brush, B. A. Myers, and E. G. Tarrant, "Home Automation in the Wild: Challenges and Opportunities."
5. J. Jungwoo, S. M. Lee, and B. H. Cho, "Building an Integrated Service Management Platform for Ubiquitous Cities," 2011.
6. P. Fragkiadakis, S. O. K. S. P. A. M. C. F. J. E. W. D. E. H. S. E. K. S. L., "Ubiquitous Robust Communications for Emergency Response Using Multi-Operator Heterogeneous Networks," *EURASIP Journal on Wireless Communications and Networking*, pp. 1-16, 2011.
7. S. M. Shaheed, "Effective Smart Home System Based On Flexible Cost in Pakistan," in *The Fourth HCT Information Technology Trends (ITT 2017)*, Dubai, 2017.
8. P. Waghmare, "Survey on: Home Automation Systems," in *International Conference on Trends in Electronics and Informatics ICEI*, 2017.
9. P. P. Gaikwad, R. K. Gaikwad, and S. S. Gaikwad, "A Survey Based on Smart Home System Using Internet-of-Things," in *International Conference on Computation of Power, Energy,*

*Information and Communication*, 2015.

10. V. Yadav, A. M. S. S. B., "Smart Home Automation Using Virtue of IoT," in *2nd International Conference for Convergence in Technology (I2CT)*, 2017.
11. M. Asadullah, I. A. R. S. M. F. A. B. U. M. I., "An Overview of Home Automation Systems," Peshawar.
12. N. Komninos, S. K. A. D. I. G., "Survey in Smart Grid and Smart Home Security: Issues, Challenges, and Countermeasures," *IEEE Communication Surveys & Tutorials*, vol. 16, p. 1933, 2014.
13. P. Mongkolwat, S. N. S. S. K. B., "IoT-based LED Lighting Control in Smart Home," in *2018 IEEE International Conference on Applied System Invention (ICASI)*, 2018.
14. J. Margulies, T. G. L., "Garage Door Openers: An Internet of Things Case Study," *IEEE Security Privacy*, vol. 13, pp. 80-83, 2015.
15. F. Shhadeh, A. E. S. N., "System Architecture for Smart Home Meter," in *2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes Systems (IT-DREPS)*, 2017.
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. 2018].
17. K. Bing, A. G. B. R., "Design of an Internet of Things-based Smart Home System," in *The 2nd International Conference on Intelligent Control and Information Processing*, 2011.
18. [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. 2018].
19. AlShu'eili, H. S. A. K., "Voice Recognition Based Wireless Home Automation System," in *4th International Conference On*, Kuala Lumpur, 2011.
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.
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.
22. "Smart Home Sensors," IBM, 2016. [Online]. Available: https://www.ibm.com/blogs/internet-of-things/sensors-smart-home/.
23. R. Sharma, N. K., "Top 15 Sensor Types Being Used in IoT," [Online]. Available: https://www.finoit.com/blog/top-15-sensor-types-used-iot/.
24. M. Kuzlu, S. A., "Review of Communication Technologies for Smart Homes/Building Applications," *IEEE*, 2015.
25. F. Al-Turjman, R. B., "Small Cells in the Forthcoming 5G/IoT: Traffic."
26. F. Vafa, H. H. P., "Wireless Sensor Networks and LTE-A," in *IEEE 38th Conference On Local Computer*, 2013.
27. P. McDermott-Wells, J. W. F., "What is Bluetooth?," *IEEE Potential*, vol. 23, pp. 33-35, 2004.
28. S. Samuel, V. S. H., "A Review of Connectivity Challenges in IoT-Smart Home," in *3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, 2016.
29. S. Samuel, K. A. N., "A Review of Connectivity Challenges in IoT-Smart Home," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, 2016.
30. "Authentication Hacking: What are Authentication Hacking Attacks?," *Acunetix*, [Online]. Available: https://www.acunetix.com/websitesecurity/authentication/. [Accessed: 21 Dec. 2018].
31. O'Shea, T. P. F., "How to Prevent Identity Theft," *NerdWallet*, 4 Oct. 2018. [Online]. Available: https://www.nerdwallet.com/blog/finance/how-to-prevent-identity-theft/. [Accessed: 20 Dec. 2018].
32. "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. 2018].
33. "Smart Home: Threats and Countermeasures," *Rambus*, [Online]. Available: https://www.rambus.com/iot/smart-home/. [Accessed: 6 Dec. 2018].
34. "Two-factor Authentication," *Techopedia*, [Online]. Available: https://www.techopedia.com/definition/13699/two-factor-authentication. [Accessed: 29 Dec. 2018].

35. H. Liu, F. T. M., "Smart Solution, Poor Protection," in *IoT S&P'1*, Dallas, TX, USA, 2017.
36. P. L. R. Chze, S. M. T., "Secured IoT Gateway For Smart Nation Applications," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Limassol, 2018.
37. J. Y. Kim, S. Y. K., "Smart Home Web of Objects-based IoT Management Model and Methods for Home Data Mining," in *17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2015.
38. H. Zheng, S. M., "Modeling and Analysis of ZigBee-Based Smart Home System," in *5th International Conference on Digital Home*, 2014.
39. C., S. K., "Autonomic Computing Through Reuse of Variability Models at Runtime: The Case of Smart Homes," *Computer*, vol. 42, pp. 37-43, 2009.
40. J. H., A. T., "Security Considerations for Secure and Trustworthy Smart Home System in the IoT Environment," in *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, 2015.
41. D., N. T., "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017.
42. N. Komninos, F. G., "Survey in Smart Grid and Smart Home Security: Issues, Challenges, and Countermeasures," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 2014, pp. 1933-1954, 2014.
43. 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.
44. M. G., A. A., "Special Issue on the Theory and Practice of Differential Privacy," 2017.
45. J. Y. Kim, A. Y. S., "Smart Home Web of Objects-based IoT Management Model and Methods for Home Data Mining," in *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2015, pp. 327-331.
46. H. Z., F. K., "Modeling and Analysis of ZigBee-Based Smart Home System," in *2014 5th International Conference on Digital Home*, 2014, pp. 242-245.
47. Tyagi, A. K., Gupta, M., Aswathy, S. U., & Ved, C. (2021). Healthcare solutions for smart era: An useful explanation from user's perspective. *Recent trends in blockchain for information systems security and privacy*, 9781003139737-13.
48. Gupta, M., Ved, C., & Kumari, M. (2022). Emergence of Blockchain Applications with the 6G-Enabled IoT-Based Smart City. In *Blockchain for 6G-Enabled Network-Based Applications* (pp. 213-235). CRC Press.
49. Alazab, M., Gupta, M., & Ahmed, S. (2023). *AIoT technologies and applications for smart environments*. Institution of Engineering and Technology.
50. Gupta, M., Kumar, R., Larhgotra, A., & Ved, C. (2023). Emergence of Big Data and Blockchain Technology in Smart City. In *Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities* (pp. 83-101). CRC Press.
51. Bansal, D., Bansal, M., Tharani, K., Gupta, M., Goyal, B., & Dogra, A. (2022, October). Enhancement of smart grid technology using end-to-end reinforcement learning in deep q-network. In *AIP Conference Proceedings* (Vol. 2555, No. 1). AIP Publishing.
52. Kumar, A., Jain, R., Gupta, M., & Islam, S. M. (Eds.). (2023). *6G-enabled IoT and AI for smart healthcare: challenges, impact, and analysis*. CRC Press.