buildings

MDPI

Review

IoT—A Promising Solution to Energy Management in Smart Buildings: A Systematic Review, Applications, Barriers, and Future Scope

Mukilan Poyyamozhi [1], Balasubramanian Murugesan [1,*], Narayanamoorthi Rajamanickam [2], Mohammad Shorfuzzaman [3] and Yasser Aboelmagd [4,5,*]

[1] Department of Civil Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, India; mp6481@srmist.edu.in
[2] Department of Electrical and Electronics Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, India; narayanr@srmist.edu.in
[3] Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia; m.shorf@tu.edu.sa
[4] College of Engineering, University of Business and Technology, Jeddah 23435, Saudi Arabia
[5] Department of Mathematical Engineering, Faculty of Engineering, Alexandria University, Alexandria 21544, Egypt
* Correspondence: balamv86@gmail.com (B.M.); yasser@ubt.edu.sa (Y.A.)

Abstract: The use of Internet of Things (IoT) technology is crucial for improving energy efficiency in smart buildings, which could minimize global energy consumption and greenhouse gas emissions. IoT applications use numerous sensors to integrate diverse building systems, facilitating intelligent operations, real-time monitoring, and data-informed decision-making. This critical analysis of the features and adoption frameworks of IoT in smart buildings carefully investigates various applications that enhance energy management, operational efficiency, and occupant comfort. Research indicates that IoT technology may decrease energy consumption by as much as 30% and operating expenses by 20%. This paper provides a comprehensive review of significant obstacles to the use of IoT in smart buildings, including substantial initial expenditures (averaging 15% of project budgets), data security issues, and the complexity of system integration. Recommendations are offered to tackle these difficulties, emphasizing the need for established processes and improved coordination across stakeholders. The insights provided seek to influence future research initiatives and direct the academic community in construction engineering and management about the appropriate use of IoT technology in smart buildings. This study is a significant resource for academics and practitioners aiming to enhance the development and implementation of IoT solutions in the construction sector.

Keywords: Internet of Things; smart building; sensors; energy management; and smart home technologies

Citation: Poyyamozhi, M.; Murugesan, B.; Rajamanickam, N.; Shorfuzzaman, M.; Aboelmagd, Y. IoT—A Promising Solution to Energy Management in Smart Buildings: A Systematic Review, Applications, Barriers, and Future Scope. *Buildings* **2024**, *14*, 3446. https://doi.org/10.3390/buildings14113446

Academic Editor: Francesco Nocera

Received: 26 September 2024
Revised: 17 October 2024
Accepted: 28 October 2024
Published: 29 October 2024

1. Introduction

As urbanization intensifies, forecasts suggest that over 60% of the global population will inhabit urban areas by 2030, making the need for effective resource management in both commercial and residential structures more vital [1]. The incorporation of IoT technology into buildings provides substantial benefits, such as resource efficiency, monitoring, and management [2]. Conventional Building Automation Systems (BAS) need modification to fulfill contemporary requirements, turning into scalable, intelligent, and energy-efficient structures via the integration of IoT technology. This transition is crucial for augmenting energy efficiency, improving indoor air quality, and ensuring sustainability in business edifices [3]. As power needs escalate due to swift industrialization, IoT technologies may facilitate energy management automation [4]. Enhance user comfort and uphold air quality. Furthermore, the IoT enables uninterrupted connectivity between devices and people at

any time and location, allowing for more efficient control of energy consumption and resource use [5]. Utilizing sensor systems in a Building Management System (BMS) allows for the continuous monitoring of characteristics such as temperature, humidity, lighting, and occupancy, hence allowing maintenance engineers to enhance energy management [6]. The deployment of IoT in smart buildings integrates diverse technologies and enhances quality of life and economic growth in metropolitan areas. IoT technology is a sensor mechanism capable of detecting and recognizing data from the physical environment [7]. The IoT architecture is defined by its functionality and applications across several sectors. The IoT has four fundamental levels, each integral to the system's overall operation [8]. The first layer, referred to as the sensing layer, comprises sensors, actuators, and devices that collect data on physical and environmental parameters [9]. These components facilitate the processing and transmission of data across the network. The second tier, the network tier, includes internet/network gateways and data acquisition systems (DAS) [10]. This layer oversees data collection, conversion, and aggregation, converting analog sensor data into digital representations and linking sensor networks to the internet. It also executes critical functions such as malware protection, filtering, and data management services [11]. The third layer, known as the Data Processing Layer, serves as the processing unit of the IoT system. In intelligent buildings, data is assessed and pre-processed before transmission to the data center. This process is supervised and administered by software programs, often referred to as business applications, which enable effective data storage and administration [12]. Edge analytics is crucial for improving processing efficiency at this level. The fourth layer, referred to as the application layer, functions as the administrative platform for data. This layer employs data centers or cloud services to facilitate end-user applications across several industries, including agriculture, healthcare, aerospace, farming, and military [13]. A major difficulty in IoT technology is guaranteeing the uninterrupted connection of sensors and actuators that interact over the internet, with smart homes exemplifying the amalgamation of technology and services via home networking [14]. Figure 1 represents the layer model of IOT.

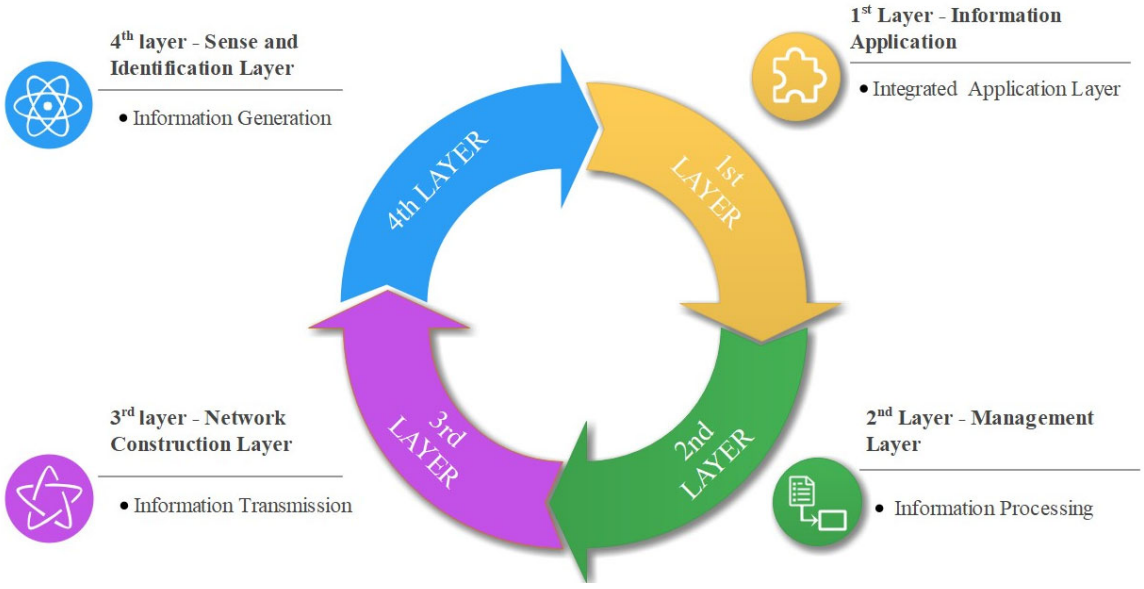

Figure 1. Four layer models for IoT.

Various solutions have been used to decrease the power consumption of IoT devices. The essential elements of the BMS are sensors that quantify characteristics such as temperature, humidity, light intensity, and occupancy [15]. The energy produced from foot traffic by piezoelectric sensors is one of the methods for power generation. Real-time energy consumption is monitored, providing insights into the operating condition of household appliances using remote monitoring devices [16]. Figure 2 depicts the components and

their linkages inside the IoT-implemented smart building. This article analyzes the basis for delivering intelligent services to customers, including energy usage monitoring, market comparison, comparative analysis, and rule-based setup. The suggested system integrates power consumption management and remote on-off control as a demonstrative example [17]. This study seeks to (i) collect relevant articles from the Scopus database utilizing primary keywords such as smart building, (IoT, sensor systems, and energy management; (ii) analyze the gathered data to identify the relationships among these keywords; (iii) assess the IoT communication protocol for sensor deployment in a smart building; and (iv) recognize the applications and challenges associated with the implementation of sensor systems and IoT in a smart building [18].

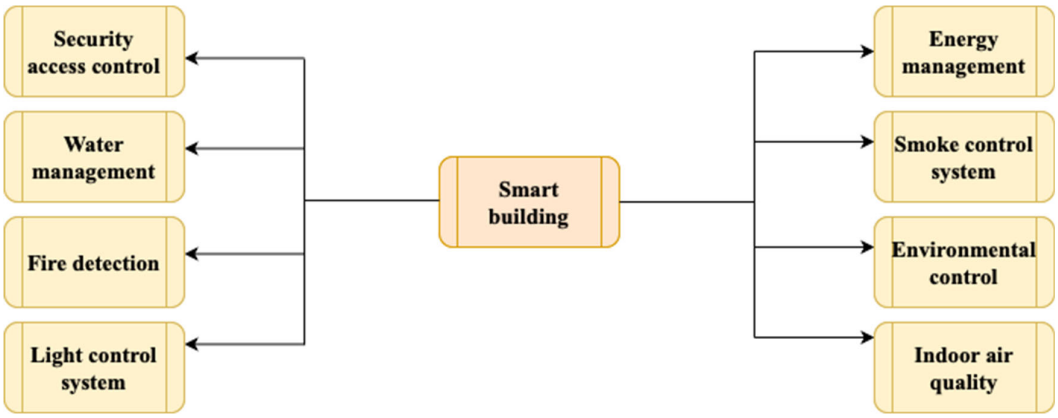

Figure 2. IoT implemented smart building.

This study examines the deficiency in incorporating IoT technology inside urban structures by emphasizing the pressing need for efficient resource management amid rising urbanization. It highlights the evolution of conventional BAS into scalable, energy-efficient frameworks via IoT integration. The study enables real-time monitoring of essential environmental factors and optimizes energy management by integrating sensor systems into BMS. Furthermore, it delineates the IoT architecture and its four fundamental levels, establishing a foundation for dependable connection among devices. The project ultimately seeks to improve user comfort, sustainability, and economic development in smart buildings via new energy management methods.

The major contributions of this review paper are

- Performs an exhaustive systematic evaluation of the available literature on IoT applications in smart buildings, essential for comprehending current trends and identifying research needs.
- Highlights the crucial impact of IoT in reducing energy consumption, especially within the construction sector, which accounts for more than 40% of worldwide energy use and greenhouse gas emissions.
- Emphasizes the uses of IoT while examining the obstacles to its adoption in smart buildings, offering a comprehensive perspective on the issues encountered in this domain.
- Proposes a structure for delivering intelligent services to users, including energy consumption monitoring and remote management of equipment, therefore augmenting the practical implementation of IoT technology.
- Offers insights and suggestions for prospective study trajectories in IoT applications in construction engineering and management, intended to assist forthcoming researchers.

2. Methodology

The analysis was carried out by collecting the research articles from Scopus, the American Society of Civil Engineers (ASCE) library, the Web of Science Library, Wiley Library, and the IEEE Library. This review is based on the research articles from 1997 to

2024. Initially, the IoT evolved in 1997, but more research has occurred in the past decade. The current research trend focuses on possible areas in a building, as shown in Table 1, and the top 15 researchers in IoT based on the citation were also categorized. Most of the literature focused on IoT communication and protocol, IoT-based tracking and monitoring technologies, IoT-controlled HVAC systems, indoor air quality monitoring using IoT technologies, and IoT-based security systems.

Table 1. Top contributors in IoT implemented smart buildings based on citations.

Author Name	Lighting and Shading Control System	IoT-Controlled HVAC System	Indoor Air Quality Monitoring	Tracking and Monitoring Using IoT Technology	IoT-Based Solar Power Monitoring	IoT For Energy Conservation	IoT-Based Security System	IoT For Power Generation	Energy Efficient	Intelligent Building
MINOLI	✓		✓						✓	✓
PLAGERAS		✓		✓	✓		✓			
LIU						✓	✓	✓		✓
EJAZ				✓		✓		✓	✓	
VERMESAN	✓	✓	✓							✓
KUMAR				✓	✓		✓	✓	✓	
YU LIANG		✓		✓	✓				✓	
SEPASGOZAR	✓				✓	✓			✓	
THIBAUD		✓	✓		✓		✓			✓
ALMUSAYLIM		✓	✓	✓				✓	✓	
SHARMA				✓	✓			✓	✓	
AL-ALI									✓	✓

✓ Authors studied or researched; ☐ Authors have not studied or researched.

Table 1 headed "Top 15 Contributors in IoT Implemented Smart Buildings Based on Citations", offers a detailed summary of the most often referenced writers in the domain of IoT related to smart building applications. Naser Hossein Motlagh is a significant contributor, with comprehensive research including several domains such as IoT-controlled HVAC systems, indoor air quality monitoring, and IoT applications for energy conservation. This extensive study demonstrates his comprehensive involvement with IoT technology. Likewise, Ethan Praga has made substantial contributions, especially in IoT-controlled HVAC systems and IoT-based smart systems, emphasizing energy efficiency and the integration of smart technologies. Conversely, José L has focused his research on IoT-based solar power monitoring, demonstrating a specific emphasis on energy-related IoT applications. Timothy Malche is distinguished for his contributions to tracking and monitoring using IoT technology, as well as IoT-based smart systems, focusing on the advancement of tracking and smart system solutions for IoT applications in intelligent buildings. Other significant contributors in Table 1 are Engr. Faiz M and Bhutta, who have concentrated on indoor air quality monitoring and IoT for power generation, underscoring their contributions to both health and energy dimensions of smart building technology. Authors such as M. Santhiya and Hamed Hellouia make substantial contributions, especially in IoT for Energy Conservation and Communication Technology and Protocols, respectively. Although writers such as Abdellah Daissaouia, Won-Suk Jang, Mobasshir, and Mahbuba M have a limited range of study subjects, their contributions are nevertheless important in the IoT smart

building sector. Table 1 illustrates the diverse levels of participation and research emphasis, with some academics contributing extensively across several IoT domains, while others concentrate on specialized, high-impact subjects such as energy saving and smart systems.

Cluster Analyses

The quantification of cluster analysis offers a thorough examination of the research environment related to IoT-enabled smart buildings. The investigation included 1146 journals, concentrating on the leading contributors in this field, determined by citation metrics. The PRISMA protocol is used to search the parameters. The following keywords are used for getting the database: Internet of things, smart building, sensors, energy management, and smart home technologies. This citation-based assessment facilitated the identification of pivotal publications that have profoundly influenced the discourse in IoT-enabled smart building research. A comprehensive keyword analysis was conducted with citation analysis, resulting in 7222 distinct terms linked to the relevant literature. Of these, 770 keywords satisfied the established relevance level, indicating a considerable diversity in study areas, including energy efficiency, automation, and sustainability in smart buildings. The substantial quantity of keywords indicates a dynamic and developing area of research, emphasizing the multidisciplinary characteristics of IoT applications in building management. Furthermore, the geographical distribution of contributions to research on IoT-implemented smart buildings was examined, indicating participation from 92 nations. Of these, 46 nations achieved the criteria for significant contributions, demonstrating a worldwide interest and investment in smart building technology. This study highlights the collaborative essence of research in this domain, as it incorporates unique viewpoints and skills from several places. The organizational landscape was evaluated, revealing 1046 entities actively involved in research on IoT-enabled smart buildings. Twenty-six organizations surpassed the threshold for significant research contributions, signifying a focused effort by specific entities to enhance knowledge and innovation in this domain. This comprehensive research underscores the significant cooperation and involvement across academic, governmental, and industrial sectors in the development of smart building solutions using IoT technology.

The IoT is revolutionizing several industries via the integration of modern technologies such as machine learning (ML), artificial intelligence (AI), and embedded systems, while also tackling issues related to data privacy and security [19]. In smart homes, the IoT interlinks devices such as thermostats, lighting systems, and security cameras, facilitating effortless management and automation. Artificial intelligence and machine learning improve user experiences by analyzing preferences and managing energy use. In agriculture, IoT sensors assess soil moisture, temperature, and crop health, use machine learning to forecast irrigation requirements, and enhance yields [20]. Autonomous drones do activities such as sowing and pest management with accuracy. Fog computing enhances IoT by facilitating data processing near the source, hence minimizing latency for essential applications such as industrial automation and healthcare [21]. Figure 3 depicts a smart building using IoT technology, highlighting the amalgamation of diverse systems, including energy management, security frameworks, and temperature regulation, which collaboratively improve efficiency and comfort. Nevertheless, the IoT encounters substantial obstacles regarding data privacy and security [22]. The proliferation of billions of linked devices heightens the potential of cyber assaults. AI-driven security procedures facilitate the monitoring of device activity and the identification of abnormalities, while encryption and authentication techniques safeguard important information [23]. Moreover, IoT is intricately linked with embedded systems, allowing real-time monitoring and predictive maintenance in industrial environments, as well as health monitoring via wearables [24]. As IoT advances, its integration with technologies such as ML, AI, fog computing, and embedded systems is essential for fostering innovation across many industries while tackling significant privacy and security concerns [25].

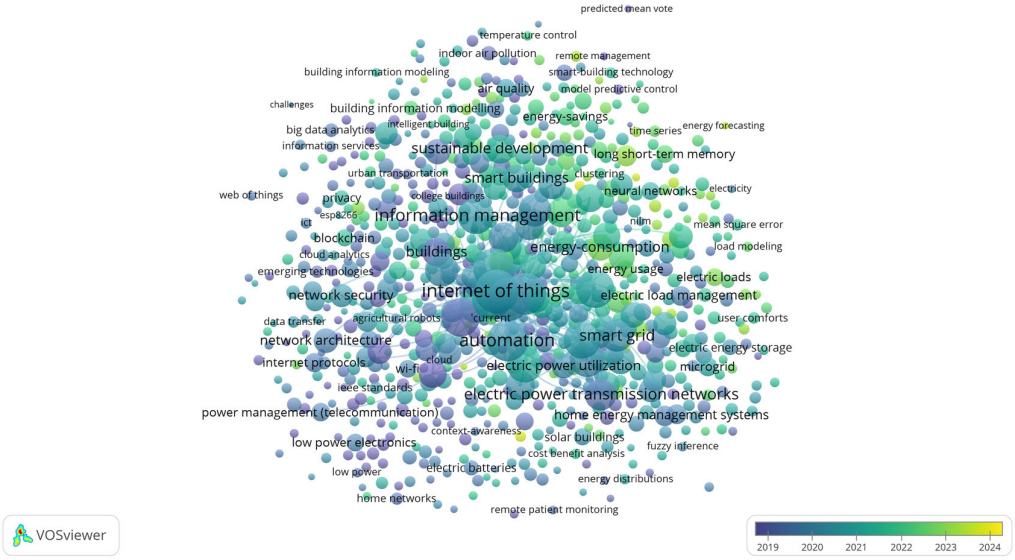

Figure 3. Key word analysis for IoT-implemented smart building.

Figure 4 illustrates the aggregation of research contributions from diverse geographical locations. This picture illustrates the substantial involvement of leading nations in the IoT, demonstrating their diverse degrees of productivity and cooperative initiatives [26]. Countries such as the United States, Germany, China, Japan, and India have emerged as prominent donors, indicative of their strong research infrastructure and investment in breakthrough technology [27]. India's rapid progress in IoT applications, especially in smart cities and agriculture, establishes it as a significant contender globally. Moreover, nations such as the United Kingdom, Canada, and South Korea are making significant contributions, underscoring the need for international cooperation in enhancing knowledge and technical progress in IoT. Figure 4 illustrates the varied research environment, highlighting how various countries together tackle global concerns and influence future research trajectories in the subject [14].

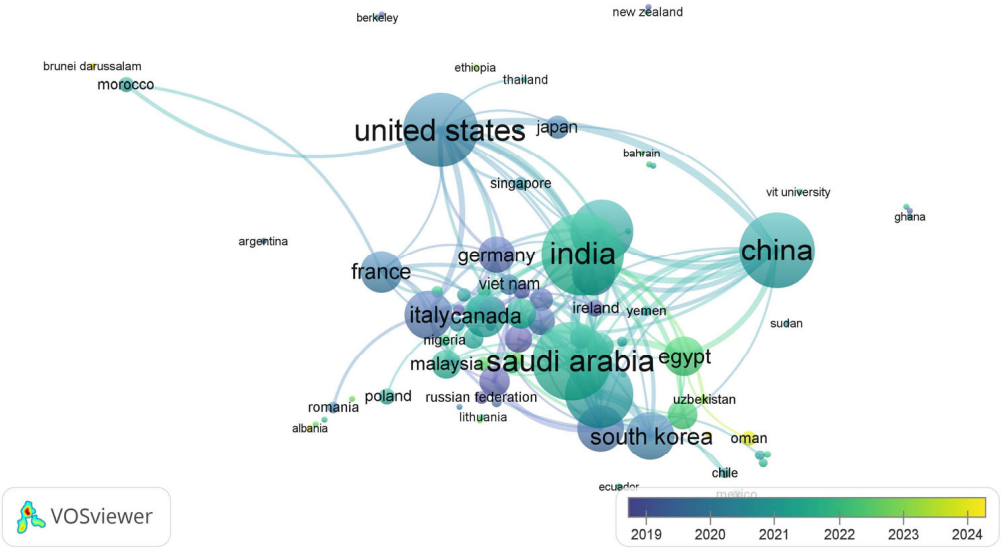

Figure 4. Countries with IoT-implemented smart building.

The Scopus database indicates that several educational fields, such as information technology, computer science, architecture, the built environment, automation, and civil and environmental engineering, are focusing on the IoT [28]. The information technology and computer science departments significantly contribute to IoT research, emphasizing

software development, data analytics, and network security. The design and built environment departments are important contributors, highlighting the incorporation of IoT technologies for intelligent buildings and urban development. Civil and environmental engineering is emerging as a burgeoning discipline within the IoT domain, focusing on sustainable infrastructure, resource management, and smart city applications. Emerging disciplines such as data science and electrical engineering are progressively integrating IoT principles, hence enhancing the multidisciplinary character of research and innovation in this sector. The contributions from these departments from 2000 to 2024 have been studied and are shown in Figure 5, highlighting their development and influence on the IoT environment.

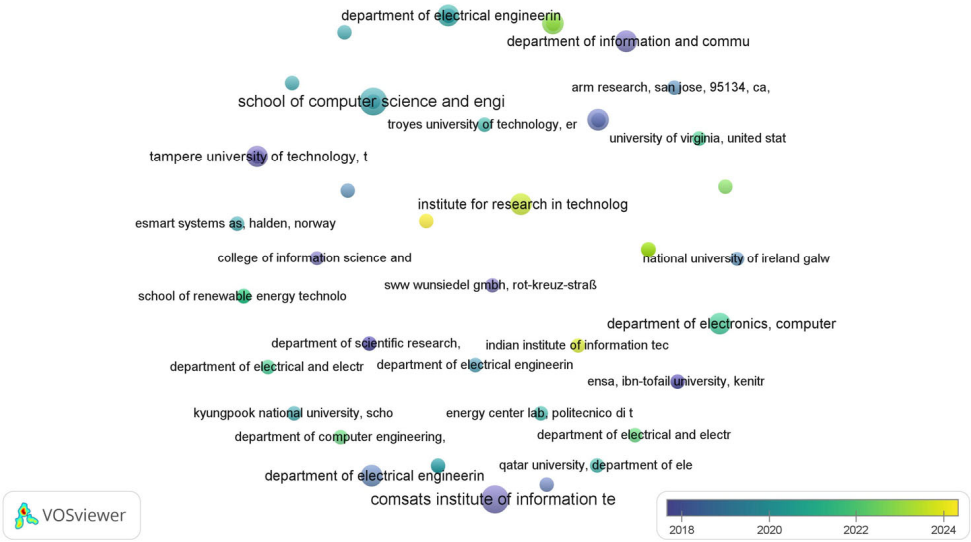

Figure 5. Organization doing research on IoT-implemented smart building.

3. Overview of IoT Technology

According to the user's point of view, a typical IoT framework comprises five significant parts of function and contribution. Sensors are the significant factor in the IoT framework that serves as a terminal; networks are the correspondence foundation; the cloud is where the information is stored; analytics, which analyzes computational and data mining; and actuators or user interfaces (administrations) [29]. The design of IoT system architecture is essential to increasing the utility of an IoT framework by linking disparate elements through the internet from any location. The architecture of the IoT framework is regularly separated on a layering premise, and numerous scientists have proposed their methods to satisfy specific necessities [30]. Some typical designs incorporate three-layers, SOA-based, middleware-based, and five-layers. It provides a large variety of tracking and monitoring of renewable energy; additionally, the functionality for industrial and domestic use of electricity, sensors, and energy sources through technology can be enhanced through the implementation of IoT [31]. IoT implementation focuses on the optimization of resources obtained by systematic analysis. IoT has innovative ways to analyze and optimize resources, ranging from elementary functions to switching off or changing various home settings or device settings to minimize energy consumption, such as light dimming [32]. This also has the potential to discover the problematic consumption that comes from issues such as outdated equipment, aging computers, or defective system components.

In an IoT-based framework, all that requires is a connection between different levels. The connectivity between the IoT gadgets, equipment, sensors, and other hardware related to the hardware control systems [33]. All devices can be tagged or connected from sensors and domestic devices to tagged livestock. Devices or applications can be linked so that they can exchange information and interpret its data. Communication can occur over short distances or medium- to long-range [34]. Big data is the product of intelligence. This

technology may be the most critical piece of manual operation, dependent on controversies concerning phenomena and automation. The position of IoT from the viewpoint of the objectives of other technology groups suits the image of the IoT [35].

IoT Communication Technology and Protocol

Wireless networking technologies are crucial for smooth communication in IoT deployment. Robust communication solutions are essential for sustaining uninterrupted connections, hence ensuring the reliable operation of IoT systems [36]. Wireless communication enables data transmission to the cloud, where it is processed to aid decision-making processes. Figure 6 shows the IoT applications for smart buildings and the protocols used for implementing IoT in a smart building. Wireless Fidelity (WiFi) is a networking system that works based on radio waves in the local area to connect gadgets based on the IEEE 802.11 Standards [37]. LTE (long-term evolution) built on GSM (Global Framework for Mobile Communications)/EDGE and UMTS/HSPA are network architectures for high-speed wireless networking [38]. The researchers reveal that the feasible protocols for IoT implementation are Low Power Large Area Network (LPWAN) technologies such as LoRa, Sigfox, and LTE-M. BLE (Bluetooth Low Energy) can be used in residential and industrial buildings for energy consumption and is less difficult to install. Related research work focuses on the value of utilizing advanced IoT communications in the energy industry, such as solar and wind power plants [39]. Based on the communication type and coverage range, the major enabling technologies are classified in Table 2. A variety of networking technologies have enabled access to the network. These technologies also use Bluetooth, NFC, RFID, xDSL, Ethernet, WiMax, USB, cellular networks, and power line communication (PLC) [40].

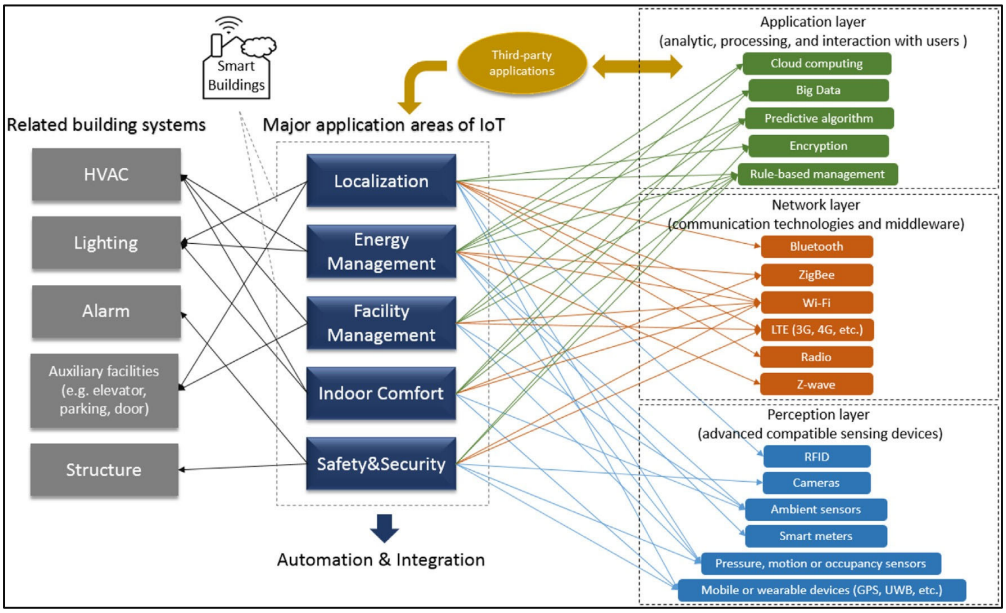

Figure 6. IoT applications for smart building and the protocols.

Although they have significant variances, MQTT, CoAP, XMPP, and HTTP are the primary IoT protocols. They are used to link IoT devices and IoT devices to the cloud. In terms of power consumption, ZigBee, (BLE), ZWave, and NFC are intended for portable devices with limited battery capacity [41]. Thus, it offers low power consumption. In terms of data rate, ZigBee, BLE, NFC, SigFox, and Z-Wave have data rates $\leq$ 1 Mbps. However, RFID has the highest data rate of 4 Mbps. In terms of range, Sig Fox and Cellular have many kilometers of coverage. 6LoWPAN, ZigBee, BLE, NFC, Z-Wave, and RFID have less than one-kilometer ranges [42]. The IEEE 802.15 working group handles the IEEE 802.15.4 short-range communication protocol, commonly used as the WSN communication

standard. Various correspondence conventions are defined for the application layer, as shown in Figure 7 [43].

Table 2. IoT Communication Technology.

S.No	Tech	Medium	Max Coverage
1	WiFi	Wireless	Up To 100 M
2	Ethernet	Copper Cable	Up To 50–70 M
3	Wi Max	Wireless	Up To 50–70 M
4	Cellular	Wireless	10–100 M
5	Xdsl	Twisted Pair Copper Cable	1.3 km
6	Plc	Electrical Power System	1500 In 100 M Between Devices

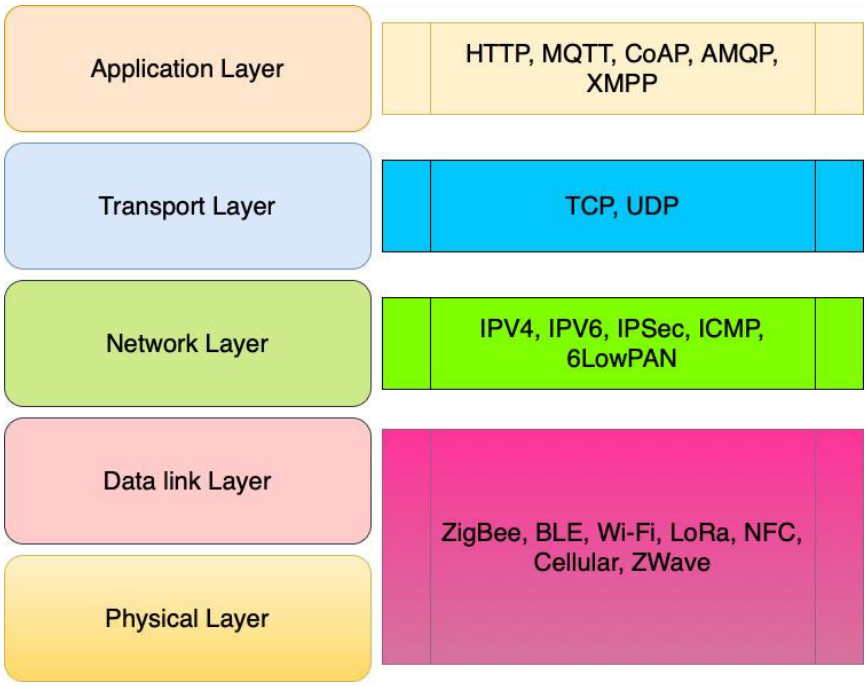

Figure 7. IoT communication protocols.

WiFi: The 2.4 GHz UHF and 5.8 GHz SHF ISM radio bands are the most widely utilized. One of the benefits of WiFi is that any device within the wireless modem's range can seek to connect to the network [44].

MQTT protocol: MQTT architecture employs a client/server approach, with each sensor acting as a client and connecting to a server. The MQTT protocol optimizes data transfer from sensor nodes to brokers over a WLAN. Customers may be required to enter a username and password to connect to MQTT brokers for security reasons [45].

CoAP protocol: CoAP is intended to meet the demands of limited-capacity devices. CoAP packets are significantly smaller than HTTP TCP streams. CoAP uses UDP rather than TCP. CoAP enables the use of Volatile Organic Compounds and multicast for addressing. CoAP uses the client/server paradigm. Clients send requests to servers, and servers respond [46].

(RFID): It is compliant with several standards, including ISO, IEC, ASTM International, the D7A, and EPC-Global. RFID systems may operate in a variety of frequency bands [41]. It works at 125–134.2 kHz for the Low-Frequency (LF) band and 13.56 MHz for the High-Frequency (HF) band. It operates at 850–960 MHz in Ultra-High-Frequency (UHF) bands where the EPC-GEN2 protocol is established [47].

BLE: BLE, often known as Bluetooth smart, is essential for IoT applications. It is optimized for IoT applications with short-range, low bandwidth, and low latency. The features of standard Bluetooth BLE include lower battery usage, faster configuration, and support for star network topology with an infinite number of nodes. Bluetooth is appropriate for smaller devices such as phones, speakers, media players, and personal computers [48].

NFC: Mobile phones, industrial applications, and contactless payment systems all make considerable use of NFC technology. Similarly, NFC improves the connecting and operation processes. In addition, control of IoT devices in various settings such as the home, factory, and workplace. NFC supports P2P network topology [49].

XMPP protocol: The XMPP protocol is a real-time information transmission specification that combines IP technology and Extensible Markup Language (XML) to provide a publish/subscribe messaging system [50].

HTTP protocol: HTTP is the foundation of the Web's client-server paradigm. HTTP is intended for one-way communication between two systems. Most IoT applications have many sensors that generate data simultaneously [51].

Zigbee: Although Zigbee has a maximum baud rate of 250 kbps, 115,200 bps was utilized for transmitting and receiving since this was the fastest speed that the microcontroller's UART could be configured to work. There is a start and stop bit for each byte sent. One of ZigBee's most important characteristics is covering huge regions with routers [52].

IPV6: IPV6, the most recent version of the IP protocol, visually shows the data information and transfers data without loss. The 0-bit compressed representation is utilized for resulting in high overlap data, providing a new approach for network viewing. IPV6 (6LoWPAN) is a network architecture that combines low-power personal wireless area networks. One of the infrastructure layer protocols supports header compression to reduce transmission overhead [53].

In smart buildings, inter-device communication is organized using a hierarchical protocol paradigm, with each tier fulfilling a distinct function. At the physical layer, protocols such as WiFi, ZigBee, Bluetooth, LoRa, and NFC provide the wireless or wired connectivity of devices, including sensors, lighting, and security systems. The data connection layer guarantees reliable transmission via the management of error detection and repair. The network layer employs protocols such as IPv4, IPv6, and 6LoWPAN to address and transport data among devices, facilitating communication across local or worldwide networks. IPSec is used to encrypt data for enhanced security. The transport layer ensures reliable data delivery between devices; TCP is used for secure communication, but UDP permits expedited transfer where dependability is not paramount, as in video streaming for security cameras. The application layer encompasses high-level protocols such as HTTP, MQTT, and CoAP, facilitating interaction and data sharing across many devices and systems inside the smart building. These protocols facilitate the seamless functioning of smart building management systems such as lighting, HVAC, and security, allowing for efficient and secure communication within the building's ecosystem.

4. Applications for IoT Technology in Smart Buildings

IoT technology in smart buildings uses sophisticated sensors, data analytics, and real-time control systems to enhance the performance and efficiency of diverse building elements. Automated climate management systems use a network of IoT sensors to monitor temperature, humidity, and occupancy levels throughout various zones of the building [54]. These sensors provide data to centralized controllers that use machine learning algorithms to dynamically modify HVAC settings, optimizing thermal comfort and energy economy. IoT-enabled thermostats may decrease HVAC output in empty rooms while preserving ideal conditions in commonly used areas, therefore reducing superfluous energy usage [55]. In intelligent lighting systems, IoT sensors identify occupancy, ambient light intensity, and the time of day to modulate artificial illumination appropriately. These systems are often combined with occupancy sensors, allowing lights to automatically deactivate when rooms

are vacant. Moreover, sophisticated IoT lighting systems may use light dimming technologies to modulate brightness in accordance with real-time data, therefore enhancing energy efficiency [56]. The amalgamation of lighting control systems with building management software offers instantaneous insights into power consumption trends, allowing facility managers to enhance energy efficiency and save operating expenses.

Security and surveillance in smart buildings are enhanced by IoT technology via networked devices, including smart cameras, motion detectors, and biometric sensors [57]. These devices interface with cloud-based systems or local servers to provide real-time video streaming, event detection, and access control. Advanced IoT surveillance systems often include AI-driven analytics, including face recognition and anomaly detection, allowing them to autonomously identify suspicious behaviors and notify security staff. Remote monitoring with mobile devices significantly improves the capacity to oversee and administer security systems from any place [58]. Energy management is a primary concern of IoT-enabled smart buildings. IoT-enabled energy meters and power use monitors consistently monitor the energy consumption of building systems, such as HVAC, lighting, and electrical devices. This data is compiled and examined via cloud computing platforms or on-site computers to detect energy inefficiencies [59]. Integrating these technologies with predictive analytics models enables smart buildings to proactively modify energy consumption patterns, improve power distribution, and diminish peak load demand. IoT systems allow the incorporation of renewable energy sources, such as solar panels, into the building's energy grid, so assuring the best use of clean energy [60].

Predictive maintenance is facilitated by IoT sensors that incessantly assess the condition of mechanical systems, including elevators, HVAC units, and electrical infrastructure. These sensors collect essential data, such as vibration levels, temperature, pressure, and wear, which are processed by predictive algorithms to identify abnormalities and probable failure areas. Predictive maintenance minimizes downtime, decreases repair expenses, and prolongs the operational lifetime of building equipment by detecting concerns prior to their escalation into breakdowns. This method is especially efficacious in large commercial edifices with intricate systems necessitating regular maintenance [61].

Occupancy monitoring uses IoT sensors, such as infrared or ultrasonic devices, to ascertain the presence and movement of individuals inside a structure. The data gathered from these sensors is analyzed instantaneously, enabling smart building systems to modify HVAC, lighting, and security configurations according to occupancy trends [62]. For example, during times of low occupancy, the building may autonomously decrease air conditioning or heating output, dim lighting, and safeguard unoccupied spaces. This real-time adjustment of building systems according to occupancy improves energy efficiency and guarantees a pleasant, responsive environment for inhabitants [63]. Ultimately, system integration using IoT technology facilitates uninterrupted communication among diverse building systems, including HVAC, lighting, security, and access control, regardless of their manufacturers. IoT systems use open communication protocols such as MQTT, BACnet, or Zigbee to guarantee interoperability across devices, establishing a cohesive control and monitoring system [64]. This cohesive strategy enables facility managers to monitor all building activities via a unified dashboard, streamlining management and facilitating coordinated reactions to fluctuations in building conditions, energy requirements, or security risks. Utilizing IoT technology, smart buildings transform into highly adaptable, energy-efficient, and user-focused environments, able to react to real-time data and predictive insights to improve overall functioning. Smart building is an essential element in the growth of cities and facilities [65]. It mainly focuses on enhancing people's comfort and safety, making maintenance easier, and increasing energy efficiency, as shown in Figure 8.

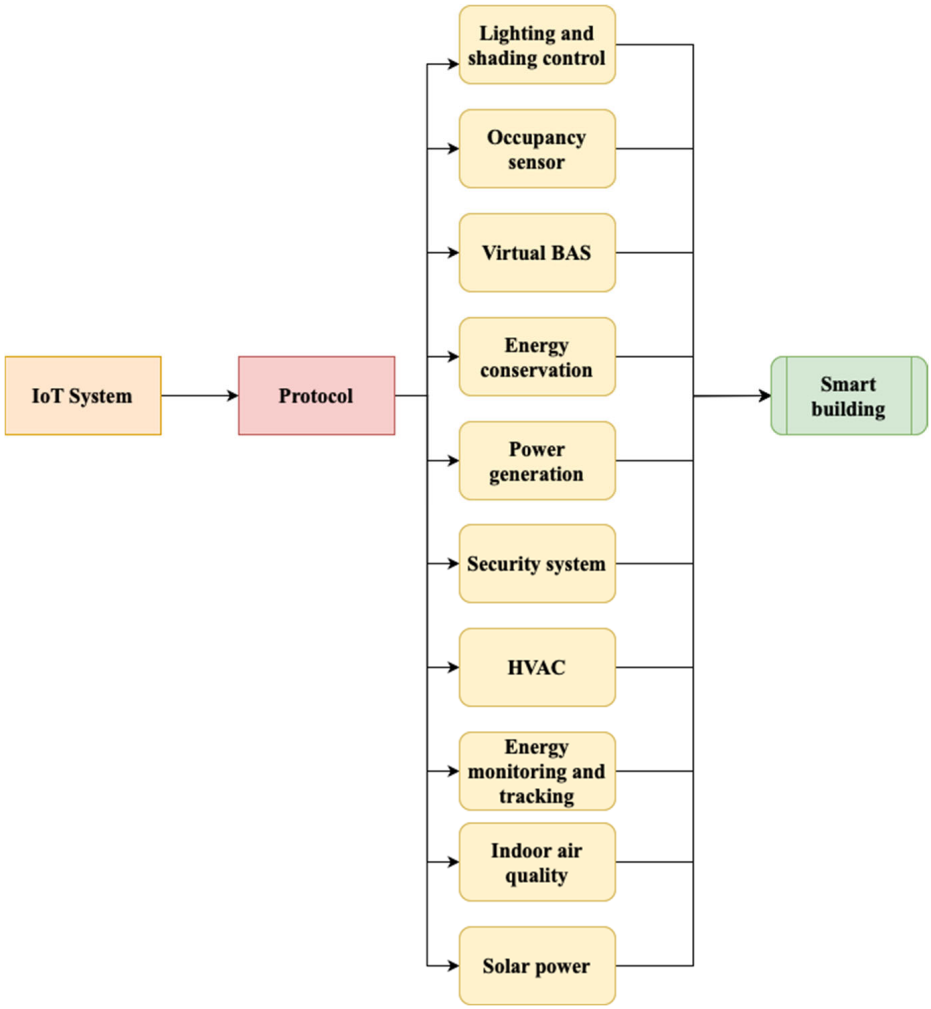

Figure 8. IoT communication for appliances.

The body of literature about the uses of IoT technology in smart buildings has been progressively expanding in recent years. The implementation of smart objects inside IoT-based infrastructures, including applications in intelligent buildings is examined [66]. The development of smart home and building solutions using IoT and cloud computing, emphasizing the practical problems encountered throughout this process [67]. A comprehensive review of Narrow Band IoT, elucidating its historical development and standardization process [68]. A blockchain-based decentralized application for the exchange of IoT sensor data, tackling many issues faced during its development [69]. In [70], a framework for the integration of vehicular clouds with the IoT to enable novel applications for smart cities, including smart households is provided. Also, a context-aware smart classroom design for intelligent campuses, highlighting the significance of technology integration [71]. In [72], examined the design of wireless sensor networks for IoT applications, emphasizing the functional design of WSNs and critical concerns pertaining to IoT architecture. Cvar et al. (2020) investigated the implementation of IoT technology in smart cities and villages, defining application areas and examining the similarities and differences between the two ecosystems [73]. Kumar et al. (2021) concentrated on the safe and energy-efficient construction of smart buildings using IoT technologies [65]. The literature study reveals an increasing interest in using IoT technology for smart buildings, with researchers investigating diverse applications, difficulties, and possible solutions within this field.

Structural Health Monitoring (SHM) has emerged as a critical study domain in recent years, focusing on improving human safety and minimizing maintenance expenses. Numerous studies have investigated the amalgamation of structural health monitoring (SHM)

with IoT technologies to establish effective and dependable monitoring systems. A structural health monitoring method based on environmental impact removal in an IoT context, using Principal Component Analysis (PCA) to mitigate environmental interferences in sensor data [74]. In [75], developed a mathematical model using piezoelectric sensors on the Pro-Trinket to monitor structural health in real-time inside an IoT framework. Similarly, a model that integrates pitch-catch and pulse-echo methodologies for damage detection in physical structures using piezoelectric sensors, validated by simulations is presented [76]. Additionally, the literature [77] introduced a framework for structural health monitoring (SHM) using IoT technologies, emphasizing intelligent and dependable monitoring systems. A comprehensive IoT structural health monitoring platform to improve human safety and decrease maintenance expenses is suggested [78]. To provide a topology maintenance monitoring system for wireless sensor networks in structural health monitoring applications, hence ensuring optimum network architecture is proposed [79]. The deployment of an Edge-SHM framework using low-power wireless sensing components for the continuous monitoring of buildings situated remote from power sources [80]. The amalgamation of IoT technologies with SHM systems presents advantageous options for effective and dependable structural health monitoring, hence augmenting human safety and diminishing maintenance expenses across diverse applications.

The integration of IoT technology enhances energy management in smart buildings by facilitating seamless communication among multiple building systems to minimize energy usage and boost sustainability (see Figure 8) [81]. The process commences with IoT devices that interconnect and communicate via defined protocols, facilitating efficient data transfer across systems. In this framework, essential elements such as lighting and shading controls, occupancy sensors, and a Virtual Building Automation System (BAS) function in unison [82]. Occupancy sensors identify the presence of persons in a place, triggering the automated modification of lighting and HVAC systems to preserve energy in unoccupied regions. Moreover, renewable energy sources, such as solar electricity, are integrated to augment power output and improve energy efficiency. Real-time energy monitoring technologies assess consumption trends, enabling proactive energy-saving strategies and enhancing indoor air quality for occupant comfort [83]. Smart buildings use IoT-driven protocols to interconnect various systems, therefore creating an intelligent, automated environment that enhances efficiency and sustainability while providing maximum comfort for inhabitants [84].

The Energy Management System (EMS) in smart buildings is essential for optimizing energy consumption, as seen in Figure 9, entitled IoT Energy Consumption for Smart Building. This detailed model illustrates the interrelated elements that constitute the energy management system. The process begins with the collection of physical measures, which are then analyzed by the EMS to enhance decision-making and actions focused on increasing energy efficiency [85]. The EMS consolidates data from several subsystems, including lighting, occupancy, heating, ventilation, air conditioning (HVAC), indoor air quality (IAQ), power management, and security systems [86]. The EMS facilitates real-time evaluation and dynamic regulation of energy parameters via the continuous monitoring of various subsystems, enabling prompt modifications to enhance performance. The several arrows in the figure represent the complex interdependencies among various components, emphasizing how their interactions together influence the building's total energy usage [87]. This framework promotes the sustainability of the smart building and improves operational efficiency via intelligent decision-making based on IoT-generated data, creating a more effective energy management environment.

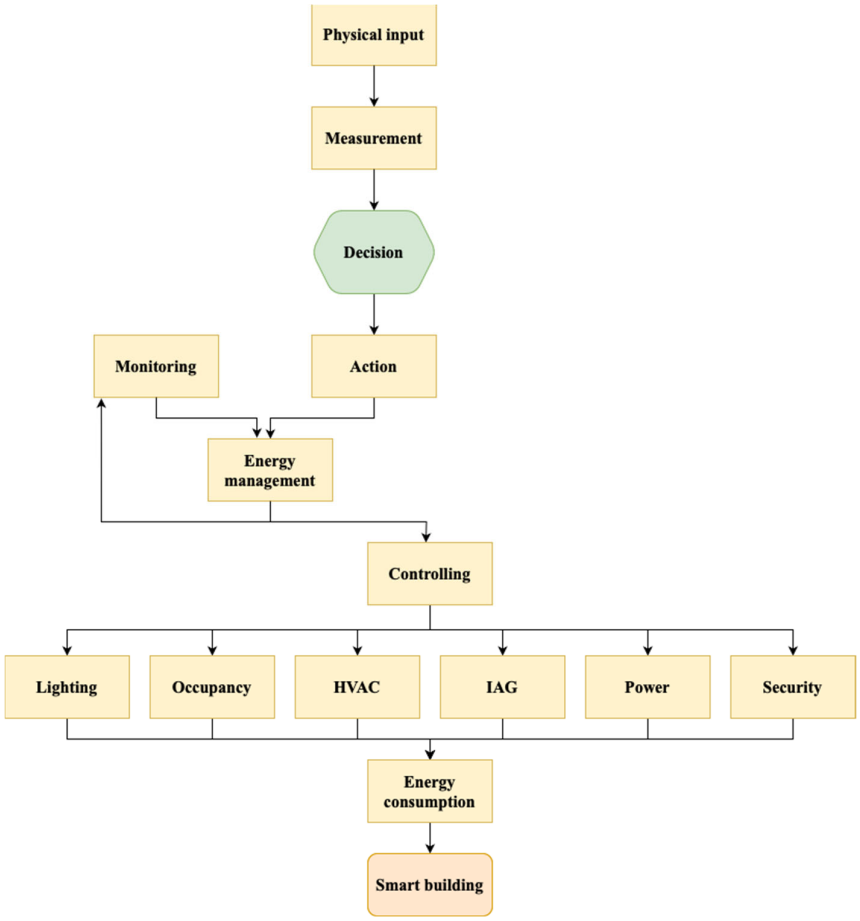

Figure 9. IoT energy consumption for smart buildings.

4.1. Lighting and Shading Control System

IoT-implemented systems are essential in controlling energy losses with the industry's trending techniques and updated technology in lighting systems. Implementing IoT-based lighting systems that inform consumers when energy usage exceeds a predetermined level within less than 100 s. The IoT devices are connected to control the light and shading of that building using the fuzzy logic method. The IoT system prototype has been developed to handle natural and artificial light inside and around the structure. Prototype studies have shown that it can maintain the desired illuminance even under high variation settings by altering shade and illumination in less than 100 s [88]. Sensor data is transferred into the primary process, which analyzes it, makes decisions, and transmits the resulting orders to the actuator subsystem. The end-user can monitor the energy consumption through HTTP server-enabled smart devices.

4.2. Energy Conservation Through Smart Occupancy Sensor

The researchers reveal that occupancy sensors for lighting can retain electrical energy up to 30% used in that building. (PIR) sensors detect the movement of living objects such as humans and animals, and they may switch actions automatically to operate the device [89]. As a result, an occupancy sensor-based lighting system ensures that lights are only turned on and off when required, with minimal disruption to routine business operations. The difference in the utilization level of the occupants concerning time in a day can be analyzed by occupancy sensors [90]. Various sensors and actuators are incorporated into the Arduino Mega to connect the building automation system to collect the data from sensors and transfer all the data to the cloud IoT server [91]. The utilization and evaluation of microwave sensors as occupancy sensors give real-time data from the environment.

4.3. IoT-Controlled HVAC System

HVAC is responsible for 40% of the total energy consumed in a building. An intelligent HVAC system offers sufficient heating, high ventilation, and a more economical air conditioning system for a facility. Smart buildings should be operated according to a layered and flexible method for offering a standard degree of interoperability across the multiple modules. HVAC energy can be measured mathematically [92]. Implementing IoT in an HVAC system is mandatory to achieve an eco-friendly working environment and conserve energy. Intelligent HVAC systems use smart thermostats, smart meters, and smartphone applications. Smart Building Energy Management System (SBEMS) describes energy utilization and predicts potential energy consumption [93]. By activating the sensors in the HVAC monitoring system, the Raspberry Pi 3 can be linked to humidity, temperature, and the current sensor. The gathered data from sensors is sent to a smartphone using the MQTT protocol on a Raspberry Pi 3, acting as a sink node. As a binary protocol, MQTT consumes very little electricity and is very small in weight [94]. Using a Wifi module as a network connection, data from sensors is sent to the cloud service, where it is stored indefinitely.

4.4. Indoor Air Quality Monitoring (IAQ)

The recent trend in the world is to create a bright and clean environment for reducing carbon footprints by 10% to 30%. IoT offers the easiest, most economical way to increase the infrastructure of the building to enable IAQ tracking in real-time [95]. Particulate Matter (PM) and Volatile Organic Compounds (VOC) Certifications are examples of current IAQ initiatives. This system establishes a method that uses evidence-based guidelines to reduce pollutant and contaminant concentrations. Arduino Uno board with ESP8266 (Espressif Systems, Shanghai, China) wireless transmission to transmit data between the devices, and Excel 2011 was used as a terminal to handle the data. Fuzzy logic rules were used to assess data from the interior environment [96]. The load was managed to utilize this information to create air quality monitoring systems that were more convenient than the threshold control systems of the past. In recent days, Blynk API (Application Programming Interface) can be installed in a building for collecting all the real-time data from sensors and the feedback from the users. This Blynk API can save up to 0.9 kWhr in the total energy consumption [97].

4.5. Virtual BAS

Smart building technology plays a significant role in the retrofit industry, especially with older buildings. IoT allows virtual BAS (Building Automation System) technologies to use cloud-based controls to handle all other HVAC systems [98]. This cloud-based controller will enforce the weekend and holiday schedules. It will also apply complicated control routines in heating/cooling zones. Modern data models such as RDF (Resource Description Framework), JSON (JavaScript Object Notation), and IFC (Industry Foundation Class) can be utilized for implementing virtual BAS in an intelligent building. Improved integration of building automation technology into the IoT is possible because of new capabilities such as more significant addresses, self-configuration, QoS measures, and security [99].

4.6. Tracking and Monitoring Using IoT Technology

Indoor built environment monitoring and control are essential for real-time tracking. The idea of intelligent building objects was proposed, and intelligent sensor nodes were used for creating facilities. Radiofrequency identification technology has been used in the civil sector since the 21st century [100]. The RFID recognizes and follows the tag attached to objects based on the electromagnetic fields. RFID labels come in two forms in particular: (1) passive tags and (2) active tags. Passive tags are connected with no energy source for identifying, whereas active RFID labels are controlled with a battery and make a more excellent detection range. RFID innovation accompanies a few constraints, particularly limited reliability and stability when the perusing system occurs through fluid or metals.

The RFID technology is based on the antenna, which exhibits the communication between the transceiver and transponder [101]. RFID framework is made out of a transceiver (called the reader) associated with an antenna and many transponders or tags, where data is collected and stored. A PC communicates with the transceiver through an application that processes the data collected by the tag. Antennas interface with the correspondence between the transceiver and transponders [102].

4.7. IoT-Based Solar Power Monitoring

IoT simplifies solar power panels' energy control and maintenance while retaining a low cost and high accuracy ratio. This IoT-based system for monitoring the solar power panels will focus on dust reduction in the panel to increase the power generation for practical usage [103]. The control of the energy generated and the cooling is refined dependent on the surface temperature by an Arduino-based detecting, controlling, and inciting framework. The IoT-based STS (Solar Panel Tracking System) can be incorporated and maintained. Depending on the new technology, a backtracking algorithm for e-tracking solar panels can be determined, and the implementation can be completed by employing IoT. The Raspberry Pi and flask framework are used to monitor the solar monitoring. Renewable energy use is shown in real-time through intelligent monitoring [104]. This aids the user in determining the amount of energy used. Impacts on renewable energy use and electrical challenges are examined.

4.8. IoT for Energy Conservation

The researchers say that around 20% of energy savings are related to the previous month's energy without energy management. Intelligent buildings with energy management systems that can regulate, track, and maximize the current energy usage of facilities. The Building Energy Management Systems (BEMS) can monitor, manage, and improve building energy use [105]. Users can remotely track and operate home appliances to conserve electricity using Zigbee wireless sensors. The framework focused on real-time energy usage mapping and building and city-scale tracking, energy efficiency measurement, and benchmarking. Zigbee is an IEEE 802.15.4-based protocol designed for low-energy, short-range communication. As a result, it is used at the network layer in various WSN frameworks. The Zigbee network layer supports star, tree, and mesh network topologies. For Zigbee, the internationally permitted ISM radio band is 2.4 GHz; however, additional frequencies are also available in different places [106]. Low cost, low power, low information rate, and self-association are all characteristics of Zigbee technology.

4.9. IoT-Based Security System

A Raspberry Pi is a single board computer that supports multiple functionalities such as home automation, security, etc. It is an embedded controller that controls the operations of sensors and other various devices connected to it. It combines all the devices through GPIO pins [107]. The researchers reveal that Raspberry Pi can be utilized as the controller. It furnishes more significant similarities with the most recent gadgets and sensors since it is the latest innovation. Especially the passive infrared sensors can be connected to the Raspberry Pi and can be utilized for home automated security systems. Also, it provides more space for future upgrades, for example, taking advantage of a tremendous quantity of the Raspberry Pi's usefulness in areas of productive power utilization via computerized light control for a much more proficient force on the board. The framework is for checking the differentiation in the energy level using IoT. Arduino has a micro-controller to peruse the sensor observations. The Arduino is connected to the current sensor and voltage divider. A USB connection connects the Arduino to the Raspberry Pi. The Raspberry Pi (RPi) serves as a server. Through RPi, the information from the Arduino will be available on the web page. The observed data is sent to the cloud through the Raspberry Pi. An open-source operating system (Raspbian, a Linux distribution) and high-level programming language (Python) can be used to capture video and photos of any moving object. Detects motion and

captures visual data recorded on a local server in our prototype project and may be accessed through a dedicated website. IoT-based home security has been built using RaspberryPi 3 and a camera from Pi-camera [108].

4.10. IoT for Power Generation

The footstep produced electricity and saved data such as produced power, stored power information, and remaining storage space gadgets. The literature determined the possibilities for generating the power using piezoelectric sensors and the different sensors associated with the framework [109]. The processor handles the gathered feedback signals and conveys consistent data to the innovative gadgets. The power generation from this technology is not continuous, and it is based on the user's corresponding footsteps. The notification can be transferred to the authorized people via mobile as an alert message when capacity arrives at its 90 to 100% limit [110]. The piezoelectric arrangement is further associated with an analog to digital converter to change over the sensors detected force changed over from the simple to the advanced yields, then the associations proceed through the ATMEL AT89552 (Microcontroller).

Implementing the IoT-based intelligent technology to tackle energy challenges in a growing society, the IoT smart energy management service has become mandatory. To maximize energy efficiency by collecting, managing, and sharing/trading information about energy utilization [111]. It is feasible to create and distribute new energy services to address national society's concerns, such as the constant rise in energy consumption, avoiding power peaks, and dealing with future trends, as shown in Figure 9. The use of IoT smart energy management services has been requisite in several settings, including smart cities and building regulations, to enhance energy efficiency and promote renewable energy sources. Utility companies increasingly mandate that residential and business customers build these systems as part of demand response programs, while governments provide incentives for their adoption. The development of energy service-oriented technology, such as M2M energy information services, facilitates automated monitoring, data analytics, and predictive maintenance. Home Energy Management Systems (HEMS) can independently control lights and appliances, improving efficiency and lowering energy expenses [112]. In summary, these IoT solutions enhance energy efficiency and facilitate sustainability objectives.

Recently, there has been an increase in interest in renewable energy in the environment, which may be achieved by adopting IoT in smart buildings. In addition to the above applications, IoT plays a role in several aspects of the energy industry, including fuel extraction, energy generation, operation, and maintenance (O and M), testing and development (T and D), as well as the final usage of energy.

4.11. Structural Health Monitoring

Structural Health Monitoring (SHM) is an advanced system that employs sensor networks, data gathering technologies, and complex algorithms to evaluate the integrity and performance of structures in real time. These systems use several sensors, including strain gauges, accelerometers, and fiber optic sensors, to assess essential factors such as strain, displacement, vibrations, and temperature [113]. The data is handled by data acquisition systems (DAS), which convert sensor inputs into digital format and synchronize the information for thorough structural evaluation [113]. Vibration-based damage detection is an essential method used in structural health monitoring (SHM), whereby alterations in modal characteristics, including natural frequencies and damping ratios, are examined to identify possible damage [114]. Modal analysis methods, such as Fast Fourier Transform (FFT), are used to transform time-domain vibration signals into frequency-domain data, therefore revealing structural alterations that may signify stiffness degradation or damage. Moreover, SHM systems often use nondestructive testing (NDT) techniques, including ultrasonic testing and acoustic emission monitoring, to identify interior flaws without inflicting harm on the structure. Machine learning technologies, such as Principal Component Analysis

(PCA) and Artificial Neural Networks (ANN), augment structural health monitoring (SHM) by detecting patterns and anomalies indicative of structural problems, hence facilitating predictive maintenance measures [115]. SHM systems use real-time monitoring via IoT integration, whereby wireless sensors relay continuous data to cloud platforms or edge devices, enabling remote oversight and immediate alarms when structural parameters surpass established limits. Finite element models (FEM) are often used with structural health monitoring (SHM) data to simulate and analyze structural responses to diverse loads, facilitating damage diagnosis and localization. The integration of these technologies enables structural health monitoring (SHM) to facilitate early identification of structural problems, enhance safety, optimize maintenance timelines, and diminish the need for expensive emergency repairs, making it a vital element of contemporary infrastructure management.

5. Barriers

The fast proliferation of IoT technology introduces a multifaceted set of issues across several disciplines. Resource consumption is a significant problem since the extensive manufacture of IoT devices hastens the depletion of scarce raw resources, hence exacerbating sustainability and availability concerns [116]. The environmental impact of these devices is exacerbated by their energy-intensive operation, which may considerably increase ecological footprints, with long-term impacts remaining mostly undetermined. The proliferation of IoT devices will further intensify electronic waste issues, with existing poor recycling rates highlighting the need for improved waste management solutions. Challenges related to integration and infrastructure, such as the effective amalgamation of various sensors and the establishment of robust network infrastructure, are crucial for the successful implementation of IoT systems. Security vulnerabilities provide a significant problem since security concerns in IoT networks, including unauthorized access and data breaches, offer hazards that need the implementation of stringent security policies [117].

The implementation of IoT in poor countries encounters technical barriers, including inadequate infrastructure and a lack of standardization, leading to compatibility challenges and inconsistent device performance. These areas also encounter social barriers since extensive rural populations lack access to essential infrastructure such as power and telephones, which are crucial for IoT systems. Moreover, policy barriers arise from the lack of regulatory frameworks, which undermines consumer trust, particularly around security and privacy concerns. Financial barriers further restrict the adoption of IoT technologies, requiring innovative models such as pay-as-you-go (PAYG) to mitigate the financial gap, while environmental barriers, including unreliable power supplies and severe weather conditions, compromise the sustainability of IoT systems in these regions. Interoperability is a significant concern since diverse IoT devices and communication protocols must interact flawlessly [118], a challenge exacerbated by differing infrastructures and standards [119]. The absence of shared infrastructures and open-source platforms hinders development and integration efforts. The absence of uniform standards across diverse devices hinders efficient data sharing. Furthermore, security challenges escalate with enhanced connection, rendering devices vulnerable to unauthorized access and data breaches, while storage management [120]. must evolve to efficiently manage the substantial volumes of data produced by IoT systems. It is essential to address these challenges for the future scalability and success of IoT technology.

The advancement of IoT technology encounters several obstacles that impede its progression. A major difficulty is the absence of interoperability and adherence to standards across suppliers [118]. To resolve this problem, entities such as the European Research Cluster on the IoT (IERC), the International Telecommunication Union (ITU), and the European Telecommunication Standards Institute (ETSI) advocate for interoperability events to ensure adherence to established standards. Security problems are an impediment to the advancement of IoT technology, especially within industrial settings [121]. The integration of IoT technologies with monitoring systems in legacy manufacturing equipment might create vulnerabilities and hazards that need thorough assessment and classification. Creating

secure IoT-enabled monitoring systems for machine tools is essential for maintaining the integrity of production processes. Furthermore, the adoption of IoT technology across several sectors, including healthcare, agriculture, and smart homes, is affected by variables such as perceived danger and financial cost [122–124]. Enhancing access to healthcare services with IoT technology may mitigate some issues and improve the efficiency of healthcare delivery. Addressing obstacles to IoT technology growth requires a multidisciplinary strategy that encompasses interoperability, security, user adoption, and the unique issues encountered by various industries and geographies. By surmounting these obstacles, IoT technology may achieve its full potential in revolutionizing many sectors and enhancing quality of life.

5.1. IoT Implementation Barriers

Despite the varied range of devices and technologies that make up the IoT, security risks must be handled on numerous levels, from tiny, implanted microchips to large high-end servers. Figure 10 illustrates a comprehensive categorization of IoT security issues. In the IoT layered architecture, security threats are separated into three categories: threats at the physical layer, threats at the network layer, and threats at the application layer. It is mandatory to note that the security threats related to IoT at various levels outlined below are not all-inclusive [125].

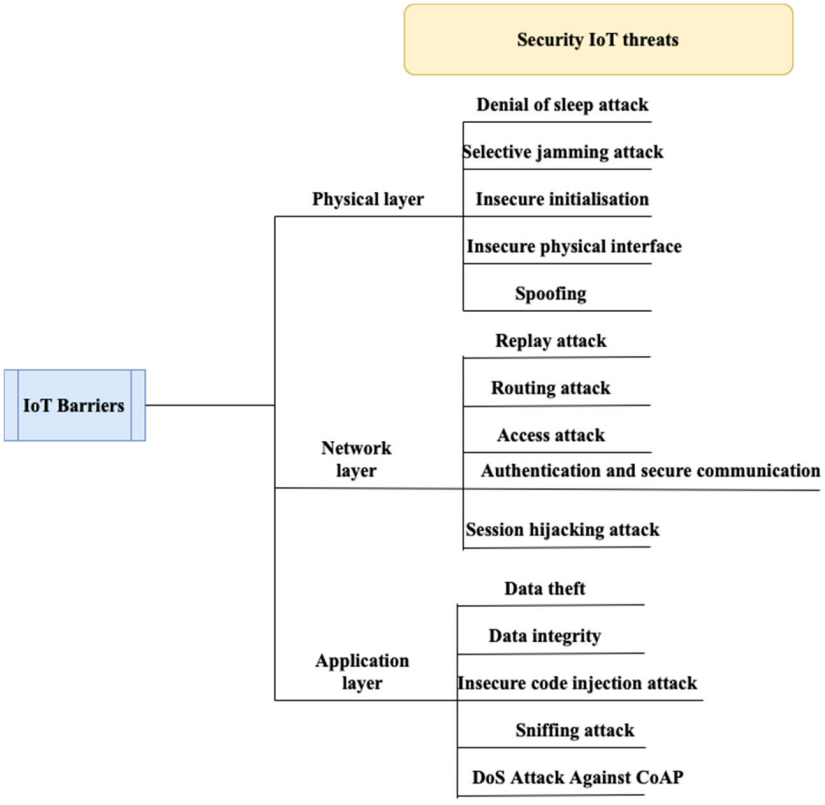

Figure 10. IoT implementation barriers and threats.

5.1.1. Physical Layer Security Threats

The sensing layer manages IoT sensors and actuators, also known as the physical layer. Sensors keep track of a wide range of physical processes in their immediate surroundings. Actuators use sensory data to accomplish a specified task in a physical situation. At the physical layer, the following critical security threats can be encountered: (1) Denial of Service (DoS): A well-known type of security attack can keep IoT devices busy receiving and processing erroneous signals, preventing them from converting to an energy-saving sleep mode and quickly draining their battery capacity. Denial-of-sleep is another name for this form of DoS attack, and it is seen as a particularly critical security issue for IoT

devices with little battery capacity. (2) Selective Jamming Attack: Jamming attacks are among the most severe and well-known DoS attacks against wireless networks. Selective jamming is more power-efficient to run and substantially more challenging to check and recognize than other jamming attacks due to the opponent's lesser exposure. (3) Insecure Initialization: Initializing and configuring IoT at the physical layer is a precautionary measure that ensures appropriate use of the entire framework while ignoring security and network service interruption. The attacker injects malicious code into the memory of the IoT devices as part of the attack. (4) Insecure Physical Interface: A few physical components work together to create real threats to IoT device functionality. Physical security flaws, programming access through physical interfaces, and testing/debugging devices have all been used to compromise network nodes. (5) Spoofing: These attacks target the weaknesses in IoT device identity validation methods. Rich countermeasures are challenging to build due to resource restrictions and the enormous number of IoT devices. The Sybil assault is a paradigm in which adversaries attempt to duplicate or counterfeit real people's identities to commit malicious behaviors and degrade IoT performance [126].

5.1.2. Network Layer Security Threats

The network layer's primary function is to get data from the physical/sensing layer to the computational unit, where it is processed. IoT connectivity, routing, and session management are among the network layer security problems described below. (i) Replay Attack: Due to its small frame size, IPv6 packet fragmentation is essential for sensing devices that conform with the IEEE 802.15.4 standard. As a result, the fragmented bits must be reconstructed at the receiving end. When malicious nodes send duplicate fragments, the receiving end encounters a buffer overflow, which causes the device to run out of resources and restart, blocking the processing of other lawful signals. (ii) Routing Attack: The IETF working group's IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) is vulnerable to a few attacks launched by weak network nodes. Wormhole attacks, in which a route is established between two nodes so that signals arriving at one node reach the other quickly, may also cause 6LoWPAN to fail. These attacks could result in eavesdropping, security breaches, and denial-of-service attacks, among other things [127].

(iii) Access attack: An access attack, also known as an advanced persistent threat (APT), is a sort of IoT network attack in which an unauthorized user or adversary gains access. For an extended period, the attacker can remain undetected in the network. (iv) Secure Communication and Authentication: IPv6 is used by IoT devices because it gives enough addresses for them to be individually identifiable. Address resolution must be made safe before transmission [128]. An identity attack may employ spoofing, deception, a Sybil attack, or impersonation. These can have a wide range of effects, from denial of service to complete control of IoT systems. As a result, fundamental management mechanisms must be used to validate IoT devices. Any vulnerability at the network layer might lead to a flood of other threats. (v) Session Hijacking Attack: A session hijacking attack allows an attacker to impersonate the target node to maintain a discussion between two nodes. Fake communications can carry out a denial-of-service attack. By changing the sequence number, the attacker sends retransmissions of message requests.

5.1.3. Application Layer Security Threats

The application layer handles and offers end-users numerous solutions in a simple approach. Smart homes, smart grids, smart cities, and other applications are part of this layer. The application layer has distinct security flaws, such as data theft and privacy risks, unlike the different layers. Below is a list of the various security vulnerabilities at the IoT application layer [129]. (a) Data Theft: Several IoT solutions, such as public healthcare monitoring, intelligent transportation systems, and smart metering, manage critical and sensitive data. Data in transit is more vulnerable to attack than data stored on IoT devices because there is so much data flowing between them. (b) Data Integrity: Maintaining data integrity in IoT networks is a significant concern. Data trust is a fundamental component

of large-scale interoperation, and the rapid progress of IoT applications has resulted in segregated data collection and interchange. Because IoT service facilities are so common, Quality of Service (QoS) has become an essential factor to consider when choosing a service. (c) Injection of Insecure Code: Insecure programming/firmware is one of the drawbacks of the IoT. In general, software/firmware updates should be completed in a secure manner. Languages such as JSON (JavaScript Object Notation), XML (Extensible Markup Language), SQLi (Structured Query Language injection), and XSS (Cross-Site Scripting) should be used with caution. (d) Sniffing Attack: The attacker uses the sniffer program to monitor network traffic in the IoT. An attacker can access personal information by monitoring network traffic if proper security measures are not applied. (e) DoS Attack on CoAP: In the IoT, the Constraint Application Protocol (CoAP) is the illegitimate application layer protocol for resource-limited devices. In the event of a DoS attack, CoAP, on the other hand, does not give any security measures for safe communications. Instead, CoAP recommends using the DTLS protocol.

6. Technical Challenges in IoT Integration for Smart Buildings

The advancement of IoT technology poses certain obstacles that must be resolved for its effective application. A significant obstacle identified in the literature is the problem of diagnostic specificity in disease management, especially with plant pathology and agriculture [130]. This dilemma highlights the need for advancing mechatronics and robotic systems to enhance disease management. A notable problem in the advancement of IoT technology is the concern of privacy and security, particularly in relation to the implementation of IoT services in libraries [131]. The paper underscores the need for addressing privacy and security issues for library directors, system designers, and IoT service consumers, emphasizing the requirement for stringent security protocols in IoT applications. Moreover, the incorporation of IoT technology into service delivery frameworks for smart cities poses issues with security vulnerabilities and potential assaults. The essay underscores the need for doing security risk assessments and recommending solutions for detected issues, accentuating the requirement for stringent security protocols in IoT-enabled smart home systems. Furthermore, the substantial increase in research and intellectual property endeavors associated with IoT technology presents difficulties in comprehending and predicting technological advancements and trends [132]. The development of sophisticated techniques for patent value is essential for understanding trends and breakthroughs in IoT technology. The literature analysis underscores several hurdles in the advancement of IoT technology, including concerns about illness management, privacy and security, smart city infrastructure, smart home security, and technological trends. Confronting these obstacles is crucial for the effective deployment and progression of IoT technology across diverse sectors.

6.1. Technological Integration

The integration of various sensing technologies in smart buildings is crucial for establishing a unified and adaptive environment. These technologies include environmental sensors, occupancy sensors, lighting control systems, and security devices, all of which must function cohesively. Nonetheless, compatibility challenges emerge from multiple communication protocols, including Zigbee, Z-Wave, WiFi, and Bluetooth, complicating smooth device connectivity. Moreover, discrepancies in data formats and architectures hinder data exchange and integration, often leading to inefficiencies. With the rise of linked devices, system complexity increases, requiring advanced management solutions to maintain seamless operation. Inadequate integration may result in operational inefficiencies, heightened energy use, and ultimately, a worse user experience in smart buildings.

6.2. Network Infrastructure

A resilient and high-capacity network infrastructure is essential for accommodating the multitude of IoT devices in smart buildings and handling the significant data they

produce. Numerous current network systems may lack the capacity to accommodate a substantial number of devices, resulting in bottlenecks that impair performance. Real-time applications, such as security monitoring and energy management, need low-latency communication since any delay or network disruption might compromise essential services. Moreover, the substantial amount of data generated by IoT devices requires sophisticated data management systems to guarantee efficient flow and processing. Insufficient network infrastructure may impede the performance of IoT applications, hence impacting operational efficiency and user pleasure.

6.3. Instruction for Users

The successful implementation of IoT technologies in smart buildings depends on users possessing a comprehensive awareness of the functionality and advantages of these systems. Nonetheless, many prospective users may be unfamiliar with IoT technology, resulting in underutilization or improper usage of the existing devices. Resistance to change is a substantial obstacle, as people may see new technology as intricate or have apprehensions over privacy and security. Creating comprehensive training programs that are both accessible and interesting may be resource-demanding and difficult to execute. Insufficient education and training may hinder the full realization of IoT technologies' potential advantages, hence restricting the efficacy of smart building systems.

6.4. Concerns Regarding Sustainability

With the proliferation of IoT technologies, it is essential to evaluate their environmental effects and prioritize sustainability in their development and implementation. The production, use, and disposal of IoT devices add to their total carbon footprint, requiring initiatives to mitigate this effect. Moreover, it is essential that the materials and energy used in IoT devices be sustainable and recyclable for enduring environmental stewardship. Smart building technologies should be designed to enhance energy efficiency while preserving functionality, hence supporting overarching sustainability objectives. Disregarding these sustainability factors may result in detrimental environmental effects, compromising the integrity of IoT devices and perhaps provoking regulatory repercussions.

6.5. Safety and Confidentiality

The growing prevalence of connected devices in smart buildings presents substantial security and privacy issues, making the safeguarding of sensitive user data essential. Every connected device constitutes a potential vulnerability for cyberattacks, requiring robust security protocols that can adapt to the changing threat environment. Moreover, IoT devices often accumulate extensive personal data, and guaranteeing the safe storage and processing of this information is a considerable difficulty. Compliance with data protection requirements, such as GDPR, complicates the development and implementation of IoT devices. Neglecting to resolve these security and privacy concerns may lead to data breaches, erosion of customer confidence, and even legal consequences that compromise the entire integrity of IoT solutions.

6.6. Obstacles to Connectivity

Numerous places, especially in developing nations, have substantial connection obstacles owing to insufficient internet and telecommunications infrastructure. The absence of consistent connectivity hinders the formation of stable connections for IoT devices, hence restricting the efficacy and scope of IoT applications. Inadequate telecommunications networks may obstruct the implementation of IoT solutions, particularly in rural or underdeveloped regions, while elevated deployment costs for securing dependable connections may pose a significant barrier to entry for several projects. Moreover, environmental elements such as physical barriers or electromagnetic interference might impede connection, exacerbating the issue. Tackling these connection difficulties is crucial to guaranteeing that IoT solutions provide their intended advantages to consumers.

6.7. Absence of Regional Proficiency

The effective adoption and upkeep of IoT systems in smart buildings depend significantly on proficient professionals capable of designing, operating, and troubleshooting these technologies. Nevertheless, a frequent lack of local competence in IoT technology impedes the implementation and longevity of several initiatives. Developing a proficient workforce necessitates investment in educational and training initiatives, which may not be universally available or accessible across all locations. Furthermore, maintaining and disseminating knowledge among team members may be difficult, especially in rapidly changing technology environments. A deficiency of local experience may result in project failures, heightened operating expenses, and dependence on foreign consultants, which may become unsustainable over time.

6.8. Ecological Issues

IoT systems are often implemented in many environmental circumstances, which may considerably impact their performance and durability. Devices must work in severe circumstances, including excessive temperatures and humidity, which may affect performance and dependability. In several areas, dependable power sources may be absent, requiring the use of alternative energy solutions, such as solar power or energy-collecting systems, to maintain operations. Moreover, gadgets must be engineered to endure environmental conditions, hence elevating manufacturing costs and complexity. Environmental issues may constrain the application of IoT solutions in certain geographies and climates, thus limiting market reach and efficacy.

6.9. Socioeconomic Inequalities

Disparities in income and resource accessibility hinder the fair implementation of IoT technologies, especially in smart buildings. Disparities between urban and rural regions may lead to an inequitable distribution of IoT advantages, with marginalized people often missing access to essential technologies and infrastructure. The elevated expenses linked to IoT solutions may preclude low-income demographics from reaping the advantages of these innovations. Moreover, including various populations and addressing their requirements in IoT initiatives is crucial for effective deployment. Neglecting social and economic gaps may exacerbate the marginalization of vulnerable communities, hence hindering the capacity of IoT to effectuate good change and enhance quality of life.

6.10. Regulatory and Policy Obstacles

The fast development of IoT technology sometimes surpasses the establishment of suitable legal frameworks, resulting in possible security risks and privacy issues. The lack of explicit norms and standards may lead to discrepancies in device security, data management, and user privacy safeguards, thus hindering innovation. Formulating complete regulations that reconcile innovation with security and privacy requirements requires coordination among stakeholders, including governmental entities, industry representatives, and civil society. Furthermore, diverse nations may possess distinct legislative frameworks, hindering the implementation of IoT technologies on a worldwide scale. Insufficient regulation may hinder innovation, result in uneven user experiences, and expose consumers to considerable security threats.

6.11. Interoperability

Facilitating efficient communication and data sharing across varied devices in smart buildings is a significant problem owing to the existence of disparate protocols and technologies. The presence of many communication protocols might result in silos, preventing devices from different manufacturers from communicating or collaborating effectively. Despite continuous initiatives to establish standards such as IEEE 802.15.4 and Matter, achieving broad acceptance continues to pose a hurdle. Moreover, disparate devices may use distinct data formats, complicating integration and analysis. The absence of compatibil-

ity may impede the operation of IoT devices, limiting the overall efficacy and efficiency of smart buildings.

6.12. Data Administration

The substantial amount of data produced by IoT devices requires sophisticated data management solutions for proper handling and analysis. Identifying suitable storage options that can expand with data expansion while ensuring accessibility is crucial for extracting insights from this data. Numerous applications need real-time data analysis for prompt decision-making, requiring substantial processing capacity and effective algorithms. Moreover, safeguarding data throughout its lifecycle—encompassing collection, storage, and transmission is essential for ensuring user privacy and adhering to rules. Inadequate data management may result in operational inefficiencies, missed insights, and even data breaches, compromising the overall efficacy of smart building systems.

6.13. Adoption by Consumers

The efficacy of IoT technology in smart buildings depends on customer interest and perceived value, necessitating the promotion of adoption among end-users. A lack of comprehensive understanding of the advantages of IoT technology among customers may result in hesitance to embrace these systems. Moreover, consumers may find IoT systems complex or daunting, thus hindering participation. Cost factors significantly influence consumer behavior, as individuals often evaluate expenses relative to possible advantages; if immediate value is not seen, adoption rates may stay low. Insufficient consumer acceptance may impede innovation and investment in IoT technology, obstructing the advancement of smart building efforts and limiting their potential effect.

6.14. Infrastructure Constraints

The effective use of IoT technology in smart buildings is contingent upon the presence of a resilient infrastructure to provide connection and functioning. Current infrastructure may need substantial enhancements to accommodate the increased demand generated by IoT devices, which may be both expensive and logistically complex. The cost obligation of creating and maintaining the requisite infrastructure might hinder several enterprises seeking to adopt IoT technologies. Moreover, maintaining infrastructure in a current and operational state requires continual investment in maintenance and enhancements. Insufficient infrastructure may restrict the scalability and efficacy of IoT solutions, consequently obstructing the advancement of smart buildings and the attainment of their advantages.

7. Conclusions

The integration of IoT technology in smart buildings presents a transformative solution for energy management, driving significant improvements in energy efficiency, operational cost reduction, and occupant comfort. The paper emphasizes the potential presented by IoT, which allows for intelligent data-driven decisions through real-time monitoring and advanced control systems. Indeed, by using energy, a 30% reduction is possible, and with operational costs, up to a 20% reduction is possible; however, several challenges remain. Some of the challenges relate to high initial investments, data security issues, and complexity in system integration. These surely require tremendous coordination among all the parties involved, robust security, and simplified integration procedures. Future research and innovation should direct focus on these areas so that such challenges can be addressed, the optimum optimization of IoT frameworks can be achieved, and its application scope in smart building environments can be further augmented. With proper strategies and collaborations, IoT can advance building systems —increasingly sustainable and more energy efficient—as this research points out. Improving energy efficiency via real-time data analytics and automated controls may result in substantial cost reductions and less environmental impact. The creation of sophisticated predictive algorithms may enhance energy consumption, hence increasing efficiency. The potential for

IoT applications cantered on user-centric design is increasing, enabling buildings to adjust to individual preferences and consequently improving occupant comfort. Moreover, the integration of IoT systems with renewable energy sources might facilitate the development of self-sustaining buildings that enhance energy resilience. As smart city projects advance, IoT-enabled buildings may enhance connectivity with extensive urban infrastructure, hence enhancing overall living circumstances. By overcoming current obstacles and using new possibilities, IoT technologies may convert smart buildings into more efficient, safe, and responsive environments for their inhabitants.

Author Contributions: Conceptualization, M.P. and N.R.; methodology, M.P.; formal analysis, M.P.; investigation, M.P.; resources, B.M.; data curation, M.S.; writing—original draft preparation, M.P.; writing—review and editing, B.M.; visualization, N.R.; supervision, B.M.; project administration, Y.A.; funding acquisition, Y.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclature

This article uses the following abbreviation.

1	API	Application Programming Interface
2	ASCE	American Society of Civil Engineering
3	ASTM	American Society for Testing and Materials
4	ATMEL	Advanced Technology for Memory and Logic
5	BAS	Building Automation System
6	BEMS	Building Energy Management Systems
7	BLE	Bluetooth Low Energy
8	BMS	Building Management System
9	CoAP	Constraint Application Protocol
10	D7A	DASH7 Alliance Protocol
11	EDGE	Enhanced Data rates for GSM Evolution
12	DoS	Denial of Service
13	EPC-GEN2	Electronic Product Code (EPC) Gen 2
14	EPC-Global	Electronic Product Code Global
15	GHZ	Gigahertz
16	GPIO	General-Purpose Input/Output
17	GSM	Global System for Mobile Communications
18	HF	High-Frequency
19	HTTP	Hypertext Transfer Protocol
20	HVAC	Heating, Ventilation and Air Conditioning
21	IAQ	Indoor Air Quality
22	IBM	International Business Machines
23	IEC	International Electro-technical Commission
24	IFC	Industry Foundation Class
25	IoT	Internet of Things
26	IPV6	Internet Protocol Version 6
27	ISO	International Organization for Standardization
28	JSON	JavaScript Object Notation
29	LoRa	Long Range Radio
30	LPWAN	Low Power Wide Area Network
31	LTE	Long Term Evolution
32	M2M	Machine to Machine
33	MHZ	Megahertz
34	MQTT	Message Queuing Telemetry Transport
35	MTC	Machine-Type Communication
36	NFC	Near Field Communication
37	P2P	Point-to-Point Topology
38	PLC	Power Line Communication

39	PM	Particulate Matter
40	QoS	Quality of Service
41	RDF	Resource Description Framework
42	RFID	Radio-Frequency Identification
43	Rpi	Raspberry PI
44	SBEMS	Smart Building Energy Management System
45	SHF	Super High Frequency
46	SOA	Service-Oriented Architecture
47	SQLi	Structured Query Language injection
48	STS	Solar panel Tracking System
49	TCP	Transmission Control Protocol
50	UDP	User Datagram Protocol
51	UHF	Ultra High Frequency
52	UMTS	Universal Mobile Telecommunications System
53	HSPA	High Speed Packet Access
54	USB	Universal Serial Bus
55	VOC	Volatile Organic Compound
56	WiFi	Wireless Fidelity
57	WIMAX	Worldwide Interoperability for Microwave Access
58	WLAN	Wireless Local Area Network
59	WSN	Wireless Sensor Network
60	xDSL	x Digital Subscriber Line
61	XML	Extensible Markup Language
62	XMPP	Extensible Messaging and Presence Protocol
63	XSS	Cross-Site Scripting

References

1. He, C.; Liu, Z.; Wu, J.; Pan, X.; Fang, Z.; Li, J.; Bryan, B.A. Future Global Urban Water Scarcity and Potential Solutions. *Nat. Commun.* **2021**, *12*, 4667. [CrossRef] [PubMed]
2. Lawal, K.; Rafsanjani, H.N. Trends, Benefits, Risks, and Challenges of IoT Implementation in Residential and Commercial Buildings. *Energy Built Environ.* **2022**, *3*, 251–266. [CrossRef]
3. O'Grady, T.; Chong, H.Y.; Morrison, G.M. A Systematic Review and Meta-Analysis of Building Automation Systems. *Build. Environ.* **2021**, *195*, 107770. [CrossRef]
4. Moudgil, V.; Hewage, K.; Hussain, S.A.; Sadiq, R. Integration of IoT in Building Energy Infrastructure: A Critical Review on Challenges and Solutions. *Renew. Sustain. Energy Rev.* **2023**, *174*, 113121. [CrossRef]
5. Bedi, G.; Venayagamoorthy, G.K.; Singh, R.; Brooks, R.R.; Wang, K.C. Review of Internet of Things (IoT) in Electric Power and Energy Systems. *IEEE Internet Things J.* **2018**, *5*, 847–870. [CrossRef]
6. Taboada-Orozco, A.; Yetongnon, K.; Nicolle, C. Smart Buildings: A Comprehensive Systematic Literature Review on Data-Driven Building Management Systems. *Sensors* **2024**, *24*, 4405. [CrossRef]
7. Jia, M.; Komeily, A.; Wang, Y.; Srinivasan, R.S. Adopting Internet of Things for the Development of Smart Buildings: A Review of Enabling Technologies and Applications. *Autom. Constr.* **2019**, *101*, 111–126. [CrossRef]
8. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035. [CrossRef]
9. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
10. Beniwal, G.; Singhrova, A. A Systematic Literature Review on IoT Gateways. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 9541–9563. [CrossRef]
11. Krishnamurthi, R.; Kumar, A.; Gopinathan, D.; Nayyar, A.; Qureshi, B. An Overview of Iot Sensor Data Processing, Fusion, and Analysis Techniques. *Sensors* **2020**, *20*, 6076. [CrossRef] [PubMed]
12. Sultana, H.P. IoT Architecture. In *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 226–238. [CrossRef]
13. Nayak, S.; Patgiri, R.; Waikhom, L.; Ahmed, A. A Review on Edge Analytics: Issues, Challenges, Opportunities, Promises, Future Directions, and Applications. *Digit. Commun. Netw.* **2024**, *10*, 783–804. [CrossRef]
14. Rafiq, I.; Mahmood, A.; Razzaq, S.; Jafri, S.H.M.; Aziz, I. IoT Applications and Challenges in Smart Cities and Services. *J. Eng.* **2023**, *2023*, e12262. [CrossRef]
15. Wang, D.; Zhong, D.; Souri, A. Energy Management Solutions in the Internet of Things Applications: Technical Analysis and New Research Directions. *Cogn. Syst. Res.* **2021**, *67*, 33–49. [CrossRef]
16. Ganesh, R.J.; Shanmugam, D.B.; Munusamy, S.; Karthikeyan, T. Experimental Study on Footstep Power Generation System Using Piezoelectric Sensor. *Mater. Today Proc.* **2021**, *45*, 1633–1637. [CrossRef]

17. Mischos, S.; Dalagdi, E.; Vrakas, D. *Intelligent Energy Management Systems: A Review*; Springer: Dordrecht, The Netherlands, 2023; Volume 56, ISBN 0123456789.
18. Rajak, P.; Ganguly, A.; Adhikary, S.; Bhattacharya, S. Internet of Things and Smart Sensors in Agriculture: Scopes and Challenges. *J. Agric. Food Res.* **2023**, *14*, 100776. [CrossRef]
19. Oliveira, F.; Costa, D.G.; Assis, F.; Silva, I. Internet of Intelligent Things: A Convergence of Embedded Systems, Edge Computing and Machine Learning. *Internet Things* **2024**, *26*, 101153. [CrossRef]
20. Magara, T.; Zhou, Y. Internet of Things (IoT) of Smart Homes: Privacy and Security. *J. Electr. Comput. Eng.* **2024**, *2024*, 7716956. [CrossRef]
21. Padhiary, M.; Saha, D.; Kumar, R.; Sethi, L.N.; Kumar, A. Enhancing Precision Agriculture: A Comprehensive Review of Machine Learning and AI Vision Applications in All-Terrain Vehicle for Farm Automation. *Smart Agric. Technol.* **2024**, *8*, 100483. [CrossRef]
22. Arshi, O.; Rai, A.; Gupta, G.; Pandey, J.K.; Mondal, S. IoT in Energy: A Comprehensive Review of Technologies, Applications, and Future Directions. *Peer-to-Peer Netw. Appl.* **2024**, *17*, 2830–2869. [CrossRef]
23. Canavese, D.; Mannella, L.; Regano, L.; Basile, C. Security at the Edge for Resource-Limited IoT Devices. *Sensors* **2024**, *24*, 590. [CrossRef] [PubMed]
24. Wu, X.; Liu, C.; Wang, L.; Bilal, M. Internet of Things-Enabled Real-Time Health Monitoring System Using Deep Learning. *Neural Comput. Appl.* **2023**, *35*, 14565–14576. [CrossRef] [PubMed]
25. Fazel, E.; Nezhad, M.Z.; Rezazadeh, J.; Moradi, M.; Ayoade, J. IoT Convergence with Machine Learning & Blockchain: A Review. *Internet Things* **2024**, *26*, 101187. [CrossRef]
26. Skopec, M.; Issa, H.; Reed, J.; Harris, M. The Role of Geographic Bias in Knowledge Diffusion: A Systematic Review and Narrative Synthesis. *Res. Integr. Peer Rev.* **2020**, *5*, 2. [CrossRef] [PubMed]
27. Savage, N. Learning the Algorithms of Power. *Nature* **2020**, *588*, 102–104. [CrossRef]
28. Singh, V.K.; Singh, P.; Karmakar, M.; Leta, J.; Mayr, P. The Journal Coverage of Web of Science, Scopus and Dimensions: A Comparative Analysis. *Scientometrics* **2021**, *126*, 5113–5142. [CrossRef]
29. Boutaba, R. The Cloud to Things Continuum. In Proceedings of the Middleware '21: Proceedings of the 22nd International Middleware Conference: Extended Abstracts, Québec City, QC, Canada, 6–10 December 2021; ISBN 9783030411091.
30. Lee, I. The Internet of Things for Enterprises: An Ecosystem, Architecture, and IoT Service Business Model. *Internet Things* **2019**, *7*, 100078. [CrossRef]
31. Giao, J.; Nazarenko, A.A.; Luis-Ferreira, F.; Gonçalves, D.; Sarraipa, J. A Framework for Service-Oriented Architecture (SOA)-Based IoT Application Development. *Processes* **2022**, *10*, 1782. [CrossRef]
32. Wang, F.; Hu, L.; Zhou, J.; Zhao, K. A Data Processing Middleware Based on SOA for the Internet of Things. *J. Sens.* **2015**, *2015*, 827045. [CrossRef]
33. Jain, S.; Choudhari, P.; Srivastava, A. *The Fundamentals of Internet of Things: Architectures, Enabling Technologies, and Applications*; Elsevier Inc.: Amsterdam, The Netherlands, 2020; ISBN 9780128196649.
34. Afonso, J.A.; Monteiro, V.; Afonso, J.L. Internet of Things Systems and Applications for Smart Buildings. *Energies* **2023**, *16*, 2757. [CrossRef]
35. Di Nardo, M.D.; Forino, D.; Murino, T. The Evolution of Man–Machine Interaction: The Role of Human in Industry 4.0 Paradigm. *Prod. Manuf. Res.* **2020**, *8*, 20–34. [CrossRef]
36. Karunarathne, G.G.K.W.M.S.I.R.; Kulawansa, K.A.D.T.; Firdhous, M.F.M. Wireless Communication Technologies in Internet of Things: A Critical Evaluation. In Proceedings of the 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Mon Tresor, Mauritius, 6–7 December 2018; pp. 1–5. [CrossRef]
37. Kanellopoulos, D.; Sharma, V.K.; Panagiotakopoulos, T.; Kameas, A. Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives. *Electronics* **2023**, *12*, 2490. [CrossRef]
38. Budka, K.C.; Deshpande, J.G.; Doumi, T.L.; Madden, M.; Mew, T. Communication Network Architecture and Design Principles for Smart Grids. *Bell Labs Tech. J.* **2010**, *15*, 205–227. [CrossRef]
39. Omrany, H.; Al-Obaidi, K.M.; Hossain, M.; Alduais, N.A.M.; Al-Duais, H.S.; Ghaffarianhoseini, A. *IoT-Enabled Smart Cities: A Hybrid Systematic Analysis of Key Research Areas, Challenges, and Recommendations for Future Direction*; Springer International Publishing: Berlin/Heidelberg, Germany, 2024; Volume 1, ISBN 4432702400.
40. Jawad, A.T.; Maaloul, R.; Chaari, L. A Comprehensive Survey on 6G and beyond: Enabling Technologies, Opportunities of Machine Learning and Challenges. *Comput. Netw.* **2023**, *237*, 110085. [CrossRef]
41. Nikolov, N. Research of MQTT, CoAP, HTTP and XMPP IoT Communication Protocols for Embedded Systems. In Proceedings of the 2020 29th International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 16–18 September 2020; pp. 18–21. [CrossRef]
42. AlShuhail, A.S.; Bhatia, S.; Kumar, A.; Bhushan, B. Zigbee-Based Low Power Consumption Wearables Device for Voice Data Transmission. *Sustainability* **2022**, *14*, 10847. [CrossRef]
43. Masoumzadeh, A.; van der Laan, H.; Dercksen, A. BlueSky: Physical Access Control: Characteristics, Challenges, and Research Opportunities. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies (SACMAT '22), Association for Computing Machinery, New York, NY, USA, 8–10 June 2022; pp. 163–172. [CrossRef]
44. Mocrii, D.; Chen, Y.; Musilek, P. IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security. *Internet Things* **2018**, *1–2*, 81–98. [CrossRef]
45. Mishra, B.; Kertesz, A. The Use of MQTT in M2M and IoT Systems: A Survey. *IEEE Access* **2020**, *8*, 201071–201086. [CrossRef]

46. Tariq, M.A.; Khan, M.; Khan, M.T.R.; Kim, D. Enhancements and Challenges in Coap—A Survey. *Sensors* **2020**, *20*, 6391. [CrossRef]
47. Dhanalakshmi, M.; Mamatha, U. RFID Based Library Management System. *Proc. ASCNT* **2009**, *3*, 227–234.
48. Raza, S.; Misra, P.; He, Z.; Voigt, T. Building the Internet of Things with Bluetooth Smart. *Ad Hoc Netw.* **2017**, *57*, 19–31. [CrossRef]
49. Yugha, R.; Chithra, S. A Survey on Technologies and Security Protocols: Reference for Future Generation IoT. *J. Netw. Comput. Appl.* **2020**, *169*, 102763. [CrossRef]
50. Ozturk, O. Introduction to XMPP Protocol and Developing Online Collaboration Applications Using Open Source Software and Libraries. In Proceedings of the 2010 International Symposium on Collaborative Technologies and Systems, Chicago, IL, USA, 17–21 May 2010; pp. 21–25. [CrossRef]
51. Chataut, R.; Phoummalayvane, A.; Akl, R. Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0. *Sensors* **2023**, *23*, 7194. [CrossRef]
52. Haque, K.F.; Abdelgawad, A.; Yelamarthi, K. Comprehensive Performance Analysis of Zigbee Communication: An Experimental Approach with XBee S2C Module. *Sensors* **2022**, *22*, 3245. [CrossRef]
53. Zhou, J.; Yang, J. Compressive Sensing in Image/Video Compression: Sampling, Coding, Reconstruction, and Codec Optimization. *Information* **2024**, *15*, 75. [CrossRef]
54. Daissaoui, A.; Boulmakoul, A.; Karim, L.; Lbath, A. IoT and Big Data Analytics for Smart Buildings: A Survey. *Procedia Comput. Sci.* **2020**, *170*, 161–168. [CrossRef]
55. Zhou, S.L.; Shah, A.A.; Leung, P.K.; Zhu, X.; Liao, Q. A Comprehensive Review of the Applications of Machine Learning for HVAC. *DeCarbon* **2023**, *2*, 100023. [CrossRef]
56. Omar, A.; Almaeeni, S.; Attia, H.; Takruri, M.; Altunaiji, A.; Sanduleanu, M.; Shubair, R.; Ashhab, M.S.; Al Ali, M.; Al Hebsi, G. Smart City: Recent Advances in Intelligent Street Lighting Systems Based on IoT. *J. Sens.* **2022**, *2022*, 5249187. [CrossRef]
57. Hakawati, B.; Mousa, A.; Draidi, F. Smart Energy Management in Residential Buildings: The Impact of Knowledge and Behavior. *Sci. Rep.* **2024**, *14*, 1702. [CrossRef]
58. Li, C.; Wang, J.; Wang, S.; Zhang, Y. A Review of IoT Applications in Healthcare. *Neurocomputing* **2024**, *565*, 127017. [CrossRef]
59. Aljohani, A. Deep Learning-Based Optimization of Energy Utilization in IoT-Enabled Smart Cities: A Pathway to Sustainable Development. *Energy Rep.* **2024**, *12*, 2946–2957. [CrossRef]
60. Karuna, G.; Ediga, P.; Akshatha, S.; Anupama, P.; Sanjana, T.; Mittal, A.; Rajvanshi, S.; Habelalmateen, M.I. Smart Energy Management: Real-Time Prediction and Optimization for IoT-Enabled Smart Homes. *Cogent Eng.* **2024**, *11*. [CrossRef]
61. Passlick, J.; Dreyer, S.; Olivotti, D.; Grützner, L.; Eilers, D.; Breitner, M.H. Predictive Maintenance as an Internet of Things Enabled Business Model: A Taxonomy. *Electron. Mark.* **2021**, *31*, 67–87. [CrossRef]
62. Fatehi Karjou, P.; Khodadad Saryazdi, S.; Stoffel, P.; Müller, D. Practical Design and Implementation of IoT-Based Occupancy Monitoring Systems for Office Buildings: A Case Study. *Energy Build.* **2024**, *323*, 114852. [CrossRef]
63. Qiang, G.; Tang, S.; Hao, J.; Di Sarno, L.; Wu, G.; Ren, S. Building Automation Systems for Energy and Comfort Management in Green Buildings: A Critical Review and Future Directions. *Renew. Sustain. Energy Rev.* **2023**, *179*, 113301. [CrossRef]
64. Ahmad, T.; Zhang, D. Using the Internet of Things in Smart Energy Systems and Networks. *Sustain. Cities Soc.* **2021**, *68*, 102783. [CrossRef]
65. Kumar, A.; Sharma, S.; Goyal, N.; Singh, A.; Cheng, X.; Singh, P. Secure and Energy-Efficient Smart Building Architecture with Emerging Technology IoT. *Comput. Commun.* **2021**, *176*, 207–217. [CrossRef]
66. Fortino, G.; Russo, W.; Savaglio, C.; Shen, W.; Zhou, M. Agent-Oriented Cooperative Smart Objects: From IoT System Design to Implementation. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *48*, 1949–1956. [CrossRef]
67. Ghayvat, H.; Mukhopadhyay, S.; Liu, J.; Babu, A.; Elahi, E.; Gui, X. Internet of Things for Smart Homes and Buildings: Opportunities and Challenges. *Aust. J. Telecommun. Digit. Econ.* **2015**, *3*, 33. [CrossRef]
68. Chen, M.; Miao, Y.; Hao, Y.; Hwang, K. Narrow Band Internet of Things. *IEEE Access* **2017**, *5*, 20557–20577. [CrossRef]
69. Ruepp, S.; Mateo, A.C.; Malarski, K.M.; Thrane, J.; Petersen, M.N. Internet of Things Connectivity in Deep-Indoor Environments. In Proceedings of the 2018 9th International Conference on the Network of the Future (NOF 2018), Poznan, Poland, 9–21 November 2018; pp. 96–100. [CrossRef]
70. Khattak, H.A.; Farman, H.; Jan, B.; Ud Din, I. Toward Integrating Vehicular Clouds with IoT for Smart City Services. *IEEE Netw.* **2019**, *33*, 65–71. [CrossRef]
71. Huang, L.S.; Su, J.Y.; Pao, T.L. A Context Aware Smart Classroom Architecture for Smart Campuses. *Appl. Sci.* **2019**, *9*, 1837. [CrossRef]
72. Yamini, B.; Pradeep, G.; Kalaiyarasi, D.; Jayaprakash, M.; Janani, G.; Uthayakumar, G.S. Theoretical Study and Analysis of Advanced Wireless Sensor Network Techniques in Internet of Things (IoT). *Meas. Sens.* **2024**, *33*, 101098. [CrossRef]
73. Cvar, N.; Trilar, J.; Kos, A.; Volk, M.; Duh, E.S. The Use of Iot Technology in Smart Cities and Smart Villages: Similarities, Differences, and Future Prospects. *Sensors* **2020**, *20*, 3897. [CrossRef] [PubMed]
74. Altabey, W.A.; Noori, M. Artificial-Intelligence-Based Methods for Structural Health Monitoring. *Appl. Sci.* **2022**, *12*, 12726. [CrossRef]
75. Elbehiery, H.M.; Hefnawy, A.A.; Elewa, M.T. Quality control enhancement via nondestructive testing for green ceramic tiles. In Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems, MWSCAS 2003, Cairo, Egypt, 27–30 December 2003; Volume 3, pp. 1130–1133. [CrossRef]

76. Abdelgawad, A.; Yelamarthi, K. Structural Health Monitoring: Internet of Things Application. In Proceedings of the 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), Abu Dhabi, United Arab Emirates, 16–19 October 2016; pp. 438–441. [CrossRef]
77. Belkeziz, R.; Jarir, Z. A Survey on Internet of Things Coordination. In Proceedings of the 2016 3rd International Conference on Systems of Collaboration (SysCo), Casablanca, Morocco, 28–29 November 2016; Volume 4, pp. 619–635. [CrossRef]
78. Mahmud, M.A.; Bates, K.; Wood, T.; Abdelgawad, A.; Yelamarthi, K. A Complete Internet of Things (IoT) Platform for Structural Health Monitoring (SHM). In Proceedings of the 2018 IEEE 4th World Forum Internet Things, Singapore, 5–8 February 2018; pp. 275–279. [CrossRef]
79. Haque, M.E.; Asikuzzaman, M.; Khan, I.U.; Ra, I.H.; Hossain, M.S.; Hussain Shah, S.B. Comparative Study of IoT-Based Topology Maintenance Protocol in Awireless Sensor Network for Structural Health Monitoring. *Remote Sens.* **2020**, *12*, 2358. [CrossRef]
80. Buckley, T.; Ghosh, B.; Pakrashi, V. Edge Structural Health Monitoring (E-Shm) Using Low-Power Wireless Sensing. *Sensors* **2021**, *21*, 6760. [CrossRef] [PubMed]
81. Akhtar, S.W.; Rehman, S.; Akhtar, M.; Khan, M.A.; Riaz, F.; Chaudry, Q.; Young, R. Improving the Robustness of Neural Networks Using K-Support Norm Based Adversarial Training. *IEEE Access* **2016**, *4*, 9501–9511. [CrossRef]
82. Domínguez-Bolaño, T.; Campos, O.; Barral, V.; Escudero, C.J.; García-Naya, J.A. An Overview of IoT Architectures, Technologies, and Existing Open-Source Projects. *Internet Things* **2022**, *20*, 100626. [CrossRef]
83. Chaudhari, P.; Xiao, Y.; Cheng, M.M.C.; Li, T. Fundamentals, Algorithms, and Technologies of Occupancy Detection for Smart Buildings Using IoT Sensors. *Sensors* **2024**, *24*, 2123. [CrossRef]
84. Lilis, G.; Conus, G.; Asadi, N.; Kayal, M. Towards the next Generation of Intelligent Building: An Assessment Study of Current Automation and Future IoT Based Systems with a Proposal for Transitional Design. *Sustain. Cities Soc.* **2017**, *28*, 473–481. [CrossRef]
85. Rodriguez-Gil, J.A.; Mojica-Nava, E.; Vargas-Medina, D.; Arevalo-Castiblanco, M.F.; Cortes, C.A.; Rivera, S.; Cortes-Romero, J. *Energy Management System in Networked Microgrids: An Overview*; Springer: Berlin/Heidelberg, Germany, 2024; ISBN 0123456789.
86. Lee, D.; Cheng, C.C. Energy Savings by Energy Management Systems: A Review. *Renew. Sustain. Energy Rev.* **2016**, *56*, 760–777. [CrossRef]
87. Lee, S.; Seon, J.; Hwang, B.; Kim, S.; Sun, Y.; Kim, J. Recent Trends and Issues of Energy Management Systems Using Machine Learning. *Energies* **2024**, *17*, 624. [CrossRef]
88. Chiesa, G.; Di Vita, D.; Ghadirzadeh, A.; Hernando, A.; Herrera, M.; Camilo, J.; Rodriguez, L. Automation in Construction A Fuzzy-Logic IoT Lighting and Shading Control System for Smart Buildings. *Autom. Constr.* **2020**, *120*, 103397. [CrossRef]
89. Samani, E.; Khaledian, P.; Aligholian, A.; Papalexakis, E.; Cun, S.; Nazari, M.H.; Mohsenian-Rad, H. Anomaly Detection in IoT-Based PIR Occupancy Sensors to Improve Building Energy Efficiency. In Proceedings of the 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2020. [CrossRef]
90. Wang, X.; Tjalkens, T.; Linnartz, J.P. Smart Office Lighting Control Using Occupancy Sensors. In Proceedings of the 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC), Calabria, Italy, 16–18 May 2017; pp. 453–458. [CrossRef]
91. Arshi, O.; Mondal, S. Advancements in Sensors and Actuators Technologies for Smart Cities: A Comprehensive Review. *Smart Constr. Sustain. Cities* **2023**, *1*, 18. [CrossRef]
92. Fazenda, P.; Veeramachaneni, K.; Lima, P.; O'Reilly, U.M. Using Reinforcement Learning to Optimize Occupant Comfort and Energy Usage in HVAC Systems. *J. Ambient Intell. Smart Environ.* **2014**, *6*, 675–690. [CrossRef]
93. Dhanalakshmi, S.; Poongothai, M.; Sharma, K. IoT Based Indoor Air Quality and Smart Energy Management for HVAC System. *Procedia Comput. Sci.* **2020**, *171*, 1800–1809. [CrossRef]
94. Masdani, M.V.; Darlis, D. A Comprehensive Study on MQTT as a Low Power Protocol for Internet of Things Application. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *434*, 012274. [CrossRef]
95. Asopa, P.; Purohit, P.; Nadikattu, R.R.; Whig, P. Reducing Carbon Footprint for Sustainable Development of Smart Cities Using IoT. In Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 361–367. [CrossRef]
96. Singh, D.; Dahiya, M.; Kumar, R.; Nanda, C. Sensors and Systems for Air Quality Assessment Monitoring and Management: A Review. *J. Environ. Manag.* **2021**, *289*, 112510. [CrossRef]
97. Bourdeau, M.; Waeytens, J.; Aouani, N.; Basset, P.; Nefzaoui, E. A Wireless Sensor Network for Residential Building Energy and Indoor Environmental Quality Monitoring: Design, Instrumentation, Data Analysis and Feedback. *Sensors* **2023**, *23*, 5580. [CrossRef]
98. Shu, L.; Mo, Y.; Zhao, D. Energy Retrofits for Smart and Connected Communities: Scopes and Technologies. *Renew. Sustain. Energy Rev.* **2024**, *199*, 114510. [CrossRef]
99. Jung, M.; Reinisch, C.; Kastner, W. Integrating Building Automation Systems and IPv6 in the Internet of Things. In Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Palermo, Italy, 4–6 July 2012; pp. 683–688. [CrossRef]
100. Yang, C.T.; Chen, S.T.; Den, W.; Wang, Y.T.; Kristiani, E. Implementation of an Intelligent Indoor Environmental Monitoring and Management System in Cloud. *Futur. Gener. Comput. Syst.* **2019**, *96*, 731–749. [CrossRef]
101. Duroc, Y. From Identification to Sensing: RFID Is One of the Key Technologies in the IoT Field. *Sensors* **2022**, *22*, 7523. [CrossRef] [PubMed]

102. Dolgui, A.; Proth, J.-M. Radio-Frequency Identification (RFID): Technology and Applications. In *Supply Chain Engineering: Useful Methods and Techniques*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 163–194. [CrossRef]
103. Rao, C.K.; Sahoo, S.K.; Yanine, F.F. A Literature Review on an IoT-Based Intelligent Smart Energy Management Systems for PV Power Generation. *Hybrid Adv.* **2024**, *5*, 100136. [CrossRef]
104. Yakut, M.; Erturk, N.B. An IoT-Based Approach for Optimal Relative Positioning of Solar Panel Arrays during Backtracking. *Comput. Stand. Interfaces* **2022**, *80*, 103568. [CrossRef]
105. Mariano-Hernández, D.; Hernández-Callejo, L.; Zorita-Lamadrid, A.; Duque-Pérez, O.; Santos García, F. A Review of Strategies for Building Energy Management System: Model Predictive Control, Demand Side Management, Optimization, and Fault Detect & Diagnosis. *J. Build. Eng.* **2021**, *33*, 101692. [CrossRef]
106. Shi, G.; Li, K. Fundamentals of ZigBee and WiFi. In *Signal Interference in WiFi and ZigBee Networks*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 9–27. [CrossRef]
107. Hercog, D.; Lerher, T.; Truntič, M.; Težak, O. Design and Implementation of ESP32-Based IoT Devices. *Sensors* **2023**, *23*, 6739. [CrossRef] [PubMed]
108. Majumder, A.J.; Izaguirre, J.A. A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; pp. 1065–1071. [CrossRef]
109. Saranya, G.; Manikandan, V.; Balaji, J.; Kandesh, M.; Karthikeyan, A. Footstep Power Generating System. *Adv. Parallel Comput.* **2021**, *39*, 49–54. [CrossRef]
110. Santhiya, M.; Keerthika, M.; Shobana, M.; Jegatha, R.; Joan, N.S.J. An IOT Used Piezoelectric Sensor Used Power Generation through Footsteps. *Mater. Today Proc.* **2020**, *37*, 166–169. [CrossRef]
111. Ganesh, P.M.J.; Sundaram, B.M.; Balachandran, P.K.; Mohammad, G.B. IntDEM: An Intelligent Deep Optimized Energy Management System for IoT-Enabled Smart Grid Applications. *Electr. Eng.* **2024**. [CrossRef]
112. Zafar, U.; Bayhan, S.; Sanfilippo, A. Home Energy Management System Concepts, Configurations, and Technologies for the Smart Grid. *IEEE Access* **2020**, *8*, 119271–119286. [CrossRef]
113. Scuro, C.; Sciammarella, P.F.; Lamonaca, F.; Olivito, R.S.; Carni, D.L. IoT for Structural Health Monitoring. *IEEE Instrum. Meas. Mag.* **2018**, *21*, 4–14. [CrossRef]
114. Civerchia, F.; Bocchino, S.; Salvadori, C.; Rossi, E.; Maggiani, L.; Petracca, M. Industrial Internet of Things Monitoring Solution for Advanced Predictive Maintenance Applications. *J. Ind. Inf. Integr.* **2017**, *7*, 4–12. [CrossRef]
115. Flah, M.; Nunez, I.; Ben Chaabene, W.; Nehdi, M.L. Machine Learning Algorithms in Civil Structural Health Monitoring: A Systematic Review. *Arch. Comput. Methods Eng.* **2021**, *28*, 2621–2643. [CrossRef]
116. Nižetić, S.; Šolić, P.; López-de-Ipiña González-de-Artaza, D.; Patrono, L. Internet of Things (IoT): Opportunities, Issues and Challenges towards a Smart and Sustainable Future. *J. Clean. Prod.* **2020**, *274*, 122877. [CrossRef] [PubMed]
117. Radoglou Grammatikis, P.I.; Sarigiannidis, P.G.; Moscholios, I.D. Securing the Internet of Things: Challenges, Threats and Solutions. *Internet Things* **2019**, *5*, 41–70. [CrossRef]
118. Palattella, M.R.; Vilajosana, X.; Chang, T.; Ortega, M.A.R.; Watteyne, T. Lessons Learned from the 6TiSCH Plugtests. In *Internet of Things. IoT Infrastructures: Second International Summit, IoT 360° 2015, Rome, Italy, October 27–29, 2015, Revised Selected Papers, Part II*; Springer: Berlin/Heidelberg, Germany, 2016; Volume 170, pp. 415–426. [CrossRef]
119. Manish, D.; Dave, K. Data Integration and Interoperability in Iot: Challenges. 2024. Manish, D.; Dave, K. Data Integration and Interoperability in IoT: Challenges, Strategies and Future Direction. *Int. J. Comput. Eng. Technol. (IJCET)* **2024**, *15*, 45–60.
120. Tong, W.; Yang, L.; Li, Z.; Jin, X.; Tan, L. Enhancing Security and Flexibility in the Industrial Internet of Things: Blockchain-Based Data Sharing and Privacy Protection. *Sensors* **2024**, *24*, 1035. [CrossRef]
121. Tedeschi, S.; Emmanouilidis, C.; Farnsworth, M.; Mehnen, J.; Roy, R. Production Management for Data-Driven, Intelligent, Collaborative, and Sustainable Manufacturing. *Adv. Prod. Manag. Syst.* **2017**, *513*, 391–398. [CrossRef]
122. Ben Arfi, W.; Ben Nasr, I.; Khvatova, T.; Ben Zaied, Y. Understanding Acceptance of EHealthcare by IoT Natives and IoT Immigrants: An Integrated Model of UTAUT, Perceived Risk, and Financial Cost. *Technol. Forecast. Soc. Chang.* **2021**, *163*, 120437. [CrossRef]
123. Wang, S.C.; Lin, W.L.; Hsieh, C.H. To Improve the Production of Agricultural Using IoT-Based Aquaponics System. *Int. J. Appl. Sci. Eng.* **2020**, *17*, 207–222. [CrossRef]
124. Ruslan, A.H.; Jusoh, A.Z.; Asnawi, A.L.; Othman, M.D.R.; Abdul Razak, N.I. Development of Multilanguage Voice Control for Smart Home with IoT. *J. Phys. Conf. Ser.* **2021**, *1921*, 012069. [CrossRef]
125. Swamy, S.N.; Jadhav, D.; Kulkarni, N. Security threats in the application layer in IOT applications. In Proceedings of the 2017 International Conference on i-SMAC (iot in social, mobile, analytics and cloud) (i-SMAC), Palladam, India, 10–11 February 2017; pp. 477–480.
126. Pourrahmani, H.; Yavarinasab, A.; Monazzah, A.M.H.; Van Herle, J. A Review of the Security Vulnerabilities and Countermeasures in the Internet of Things Solutions: A Bright Future for the Blockchain. *Internet Things* **2023**, *23*, 100888. [CrossRef]
127. Nait-Abdesselam, F.; Bensaou, B.; Taleb, T. Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks. *IEEE Commun. Mag.* **2008**, *46*, 127–133. [CrossRef]
128. Geng, H. *Internet of Things and Data Analytics Handbook*; John Wiley & Sons: Hoboken, NJ, USA, 2017; pp. 1–776. [CrossRef]
129. Mohamed, K.S. *The Era of Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 93–111. [CrossRef]

130. Ampatzidis, Y.; De Bellis, L.; Luvisi, A. IPathology: Robotic Applications and Management of Plants and Plant Diseases. *Sustainability* **2017**, *9*, 1010. [CrossRef]
131. Hahn, J. *Library Technology Reports Expert Guides to Library Systems and Services THE INTERNET OF THINGS*; American Library Association: Chicago, IL, USA, 2017; Volume 53, ISBN 9780838959848.
132. Trappey, A.J.C.; Trappey, C.V.; Govindarajan, U.H.; Sun, J.J.H. Patent Value Analysis Using Deep Learning Models-the Case of Iot Technology Mining for the Manufacturing Industry. *IEEE Trans. Eng. Manag.* **2021**, *68*, 1334–1346. [CrossRef]