sustainability

MDPI

Review

An Overview of the Architecture of Home Energy Management System as Microgrids, Automation Systems, Communication Protocols, Security, and Cyber Challenges

Kamran Taghizad-Tavana [1], Mohsen Ghanbari-Ghalehjoughi [1], Nazila Razzaghi-Asl [1], Sayyad Nojavan [2,*] and As'ad Alizadeh [3]

[1] Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz 5166616471, Iran
[2] Department of Electrical Engineering, University of Bonab, Bonab 5551761167, Iran
[3] Department of Civil Engineering, College of Engineering, Cihan University-Erbil, Erbil 44001, Iraq
* Correspondence: sayyad.nojavan@ubonab.ac.ir

Abstract: Today, the role of smart machines in our lives is valuable. With the advancement of digital technologies, such as the internet of things (IoT), many embedded systems have been developed for various applications. In homes, all daily activities and even security depend on machines. Therefore, implementing IoT-based smart homes has become a prominent research field. Also, since we are in the era of endless growth of the IoT and its applications, the topic of home automation systems is becoming more popular due to its countless advantages. In general, most home automation systems focus on one function: the ability to control home appliances remotely. In the world of information technology, the creation of rules and standards should always be done in the early stages of development because, after the work is done, incompatibilities between devices are created, which is a severe challenge and limits the use of technology. Therefore, the research on IoT technology has led to the formation of various protocols; this article gives an overview of seven essential protocols. Also, in this review article, energy consumption management, and privacy and security issues are discussed, and smart homes are introduced as critical requirements for the evolution of smart cities.

Keywords: Wi-Fi; Z-wave; Zig-Bee; bluetooth; wireless technologies; internet of things (IoT); home automation; home energy management systems (HEMS); 5G; 6LoWPAN; LoRaWAN

Citation: Taghizad-Tavana, K.; Ghanbari-Ghalehjoughi, M.; Razzaghi-Asl, N.; Nojavan, S.; Alizadeh, A. An Overview of the Architecture of Home Energy Management System as Microgrids, Automation Systems, Communication Protocols, Security, and Cyber Challenges. *Sustainability* **2022**, *14*, 15938. https://doi.org/10.3390/su142315938

Academic Editors: J. C. Hernandez and Mouloud Denai

Received: 5 November 2022
Accepted: 21 November 2022
Published: 29 November 2022

1. Introduction

Home automation, or building management systems, has been created to improve the quality of human life based on a flexible environment with high security. Therefore, home automation is becoming widespread with the emergence of new smart devices [1,2]. A reliable and suitable home automation system changes the quality of human life at an unprecedented speed. With home automation, there is no need for users to perform daily operations. Therefore, this technology plays a significant role in saving time and energy [3]. Human–Machine Interface or HMI is a user interface that connects a human to a machine, system, or device. The term can technically be applied to any screen that allows a user to interact with a machine; however, HMI is usually used in the sense of an industrial process [4,5]. Today, HMI-related study has gone one step further and turned to the Internet, with the difference that it used to be used for communication but is now used for objects [6–8]. The IoT concept was invented by (PETER T. LEWIS in September 1985 [9,10]. In his lectures, he claimed that this technology covers a diverse range of technologies concerning sensing, networking, computing, information processing, and smart control technologies [11–14]. Thanks to the introduction of this technology, the implementation of home automation systems is becoming more popular among users; as well, this is because the IoT is the first step in making homes smart through wireless technologies [15]. Also, the

application of IoT is not limited to a specific field, and a considerable contribution of small-scale applications to large-scale applications such as e-commerce [16], coal mining [17], smart farming [18], laboratory monitoring [19], public service [20], crowd sensing [21], and many other areas have been shown, and, in general, this technology enables the monitoring and operation of devices by different methodologies in any part of the world using only an Android application. As the demand for electricity increases, smart homes have become a research area to remotely control home appliances using the IoT [22–25]. Also, the significant benefits gained from wireless sensors and nanotechnology, among others, have fundamentally changed the way information technology and communication environments work. While IoT is still a growing and expanding platform, the current research in privacy and security shows that there needs to be more integration and unification of security and privacy, which may affect user adoption of the technology because of fear of personal data exposure [26]. The last two decades have experienced a steady rise in the production and deployment of sensing-and-connectivity-enabled electronic devices, replacing "regular" physical objects. The resulting IoT will soon become indispensable for many application domains [27]. The smart home is the proper integration of information technology and services using home networks in various home appliances for the convenience of the elderly and disabled people, and generally improving the quality of life [28–30]. Smart homes will allow users to perform actions such as adjusting the temperature of the house, turning lamps on and off, etc., without any physical connection [31]. Another critical issue noted in this article is the response to demand. Energy consumption has increased significantly, causing an increase in energy demand. Companies and industries spend thousands of dollars on energy and millions of dollars to find ways to conserve energy. Therefore, saving energy is one of the main goals of all technological innovations toward energy conservation. One of the ways through which technology helps in saving energy is the home automation system based on the IoT. Home energy management systems (HEMS) are optimal for providing energy management services to effectively manage energy production, storage, and consumption in smart homes. Therefore, users can optimize energy consumption by applying schedules based on their home appliances' demand-response programs. Figure 1 shows the general architecture of a HEMS. HEMS should be more flexible in planning, managing, and controlling smart home appliances to save energy. In addition, active control services can be delivered to smart home users, such as providing accurate information about electricity consumption and energy pricing in HEMS-based smart homes. Also, users can plan and manage the service time of each smart home piece of equipment. Figure 2 shows the regular operation of a smart HEMS center with four main functions.

The communication platforms in smart homes can be divided into wireless and wired, which is fully described in Section 3. Wireless technology introduces various connections such as Bluetooth, IoT, Wi-Fi, GSM, etc., each of which has its advantages, disadvantages, applications, and specifications [32]. These connections offer home appliance control utilizing an Android app that helps overcome the disadvantages of conventional home control, although the personal computers that use them consume more energy and require more money. On the other hand, the benefit of using Android as a platform is that it is simple and easy to use. It can also use any media, such as Bluetooth, IoT, and Wi-Fi, to execute commands given by the user [33,34]. The smart home system consists of three layers of sensors, operators, and controllers. In other words, a smart building consists of a set of sensors, several operators, and a central control system; these sensors receive the appropriate information and, according to the predetermined program in the central control system, a suitable signal is placed in the output. These sensors send their communication to a central controller, and the main controller can control many operators, such as air inlet and outlet valves, electric doors, and windows. Temperature sensors and motion sensors are examples of sensors used in smart homes.

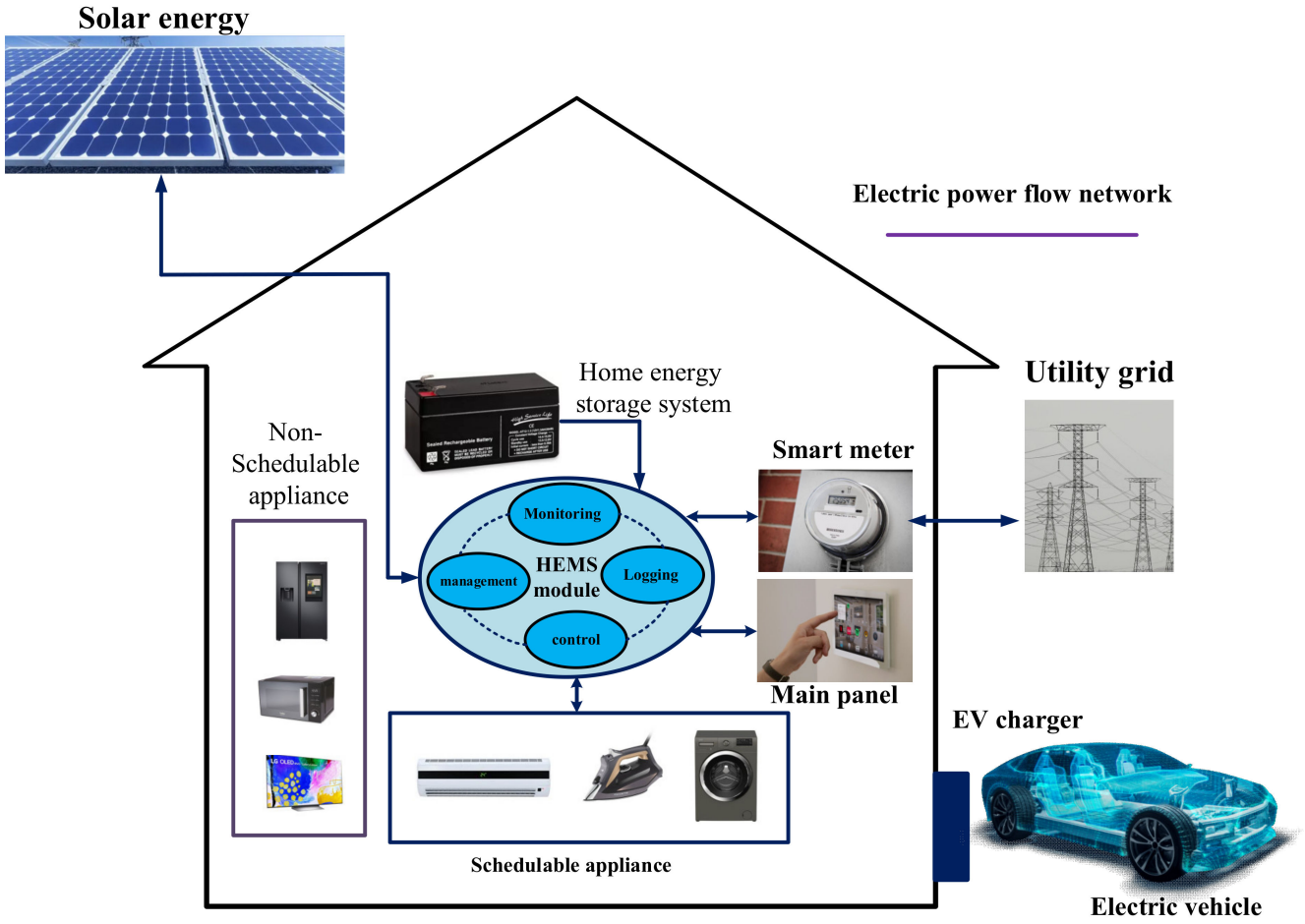

Figure 1. Overall architecture of a HEMS.

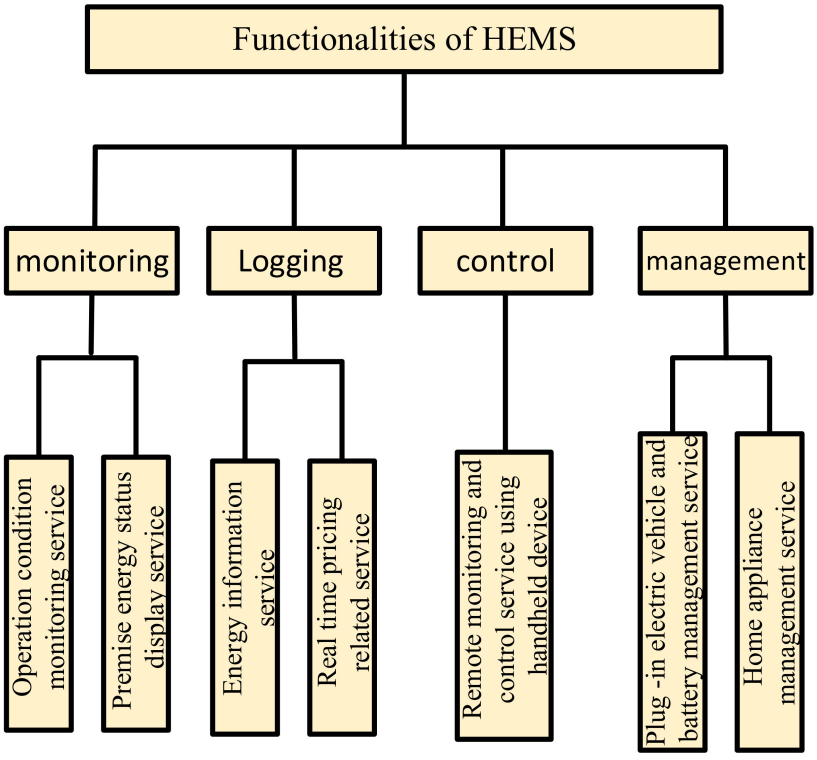

Figure 2. Functionalities of a smart HEMS.

Paper Organization

This article is organized as follows:

Section 2 shows the architecture of the home automation system. In Section 3, Communication protocols related to smart homes have been discussed. Sections 4–10, respectively, in order, represent home automation systems based on protocols (Bluetooth, Zig-Bee, Z-wave, Wi-Fi, 5G, LoRaWAN, and 6LoWPAN). In Section 11, privacy and security issues are discussed. Section 12 describes challenges in smart homes and future trends. Table 1 compares the information related to these protocols and Table 2 shows some security issues and challenges. Finally, Table 3 shows the advantages and disadvantages of the discussed protocols.

Table 1. Comparison of different protocols in smart home automation.

Protocol	Frequency	Topology	Network	Data Rate	Power Consumption	Smart Grid Application Areas	Cost Adder	Range
Zig–Bee	2.4 GHz	Star, Mesh, Cluster tree	LAN	250 kbps	Low	Energy monitoring; smart lighting; home automation;	Medium	10–300 m
Z-wave	900 MHz	Mesh	LAN	100 kbps	High	Home automation	Low	30 m
Wi-Fi	2.4, 5 GHz	Star, P2P Cluster tree	LAN	0.1–54 mbps	Medium	Home automation	Medium	50 m
Bluetooth	2.4 GHz	P2p, star	PAN	721 kbps	Very low	Home automation	Very low	3–30 m
5G	600 MHz To 6 GHz	Star	PAN	Up to 25 GbPS	Low	Distributed monitoring & control	Low	Various km
LoraWAN	433/868/780/915 MHz	Star on star	NAN; WAN	290 bps–50 kbps	Low	Equipment management; Online monitoring	Low	2.5 km urban/15 km suburban/14 km rural
6LoWPAN	2.4 GHz	Star	LAN	250 kbps	Medium	Smart metering; home automation	Medium	800 m

2. Home Automation System Architecture

As shown in Figure 3, the architecture of the home automation system consists of two main parts: the internal part on the left and the outer portion, which includes sensors, users, and services, on the right. Also, the communication manager is in contact with all sensors and actuators in its protocol, and all communication is done this way. In general, the information that enters the system is divided into three categories:

1. The device sends its service information (such as coffee);
2. Context sensors, such as light sensors, show current location information;
3. Users provide the necessary information through a user interface (for example, an interactive home screen) to make changes to specific settings.

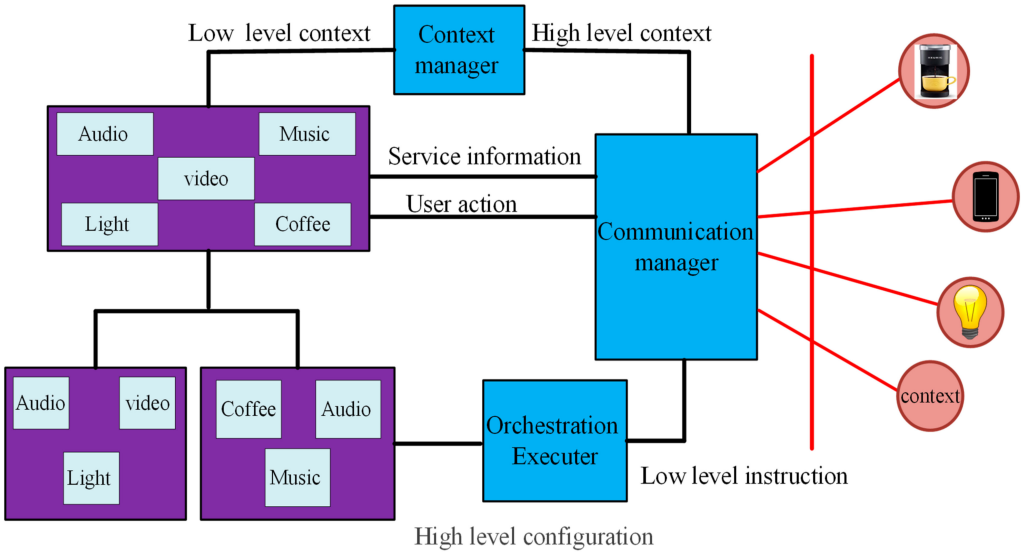

Figure 3. Home automation system architecture.

The information from the sensors (the low-level context) is sent to the Context Manager, which reasons and infers high-level context, which is then forwarded to the Composition Manager. For example, a sensor related to the Bluetooth protocol will detect a smartphone's presence. Then, the Context Manager identifies the owner of the smartphone and the location where the sensor is located (for example, the sensor is in the bedroom, and Kamran owns the smartphone). Hence, high-level context information is easily obtained (Kamran is in the bedroom). In addition to the data obtained in the high-level context, the composition manager will be able to obtain information about different system applications. Also, as seen in the Figure 3, the services that belong to the same family are grouped in a box. (e.g., light, sound, video, etc.). Therefore, smart home users can categorize new compounds in different packages based on this method. Finally, the composition needs to be enforced for the various services. The Orchestration Executor is responsible for converting the information of the different blocks into service-specific implementations. This conversion is only possible if the ontologies of the services contain enough information about their control and data flow.

3. Communication Protocols in Home Automation System

Smart home communication protocols are divided into wireless and wired groups based on the communication platform. Wired communication protocols are less diverse due to the need for peripheral hardware. One of the most significant developments in Europe in recent years in the field of smart home technology is the development of the KNX/EIB protocol for home automation [35]. KNX is an internationally recognized standard for smart home implementation and control [36]. The European Standard for Electronic Standardization (CENELEC) recently introduced the KNX standard in the EN 50,090 series, which became the international standard ISO/IEC 14,543 in July 2006 [37]. According to research, around 12 million KNX devices have been installed worldwide, more than 500,000 devices are compatible with this standard, and the organization controlling the features of this standard is formed by more than 150 members, including Siemens and Schneider. KNX enables connections using twisted pairs, power lines, and wireless and Ethernet links, and the range of sectors and applications that can benefit from this standardization is wide. There are also different types of wired protocols, such as Ethernet, X10, and UPB, which, in addition to increasing security, have disadvantages such as setup problems, incompatibility with products, and poor encryption. The emergence of the IoT has witnessed tremendous success in the application of wireless sensor networks and pervasive computing for various applications [38]. In general, wireless sensor networks have more advantages than traditional wired networks, including a high reliability, easy setup and installation, and increased productivity [39]. Also, recent electronics and wireless communication advances have made it possible to design and manufacture sensors with low power consumption, small size, reasonable price, and various applications. These small sensors can perform actions such as receiving multiple types of environmental information (based on the type of sensor), and processing and sending that information, causing people to replace traditional wired networks with wireless networks [40,41]. Of course, with the expansion of smart homes in recent years, wireless network technology has also faced challenges that have delayed its widespread adoption [42]. As shown in Figure 4, when it comes to home automation systems [43], Bluetooth [44], Zig-Bee [45], Z-wave [46], and Wi-Fi [47] are among the most widely used protocols that users use to communicate. According to the statistical graph shown, these four protocols have the largest share in terms of application compared to other protocols. Also, according to the chart, the remaining 18% includes protocols such as LoRaWAN, 5G, 6LoWPAN, etc., which will be explained below. These protocols are generally connected to devices or peer-to-peer networks. They can be used independently, share their sensor data, or, if necessary, store their data permanently on a local server save [48].

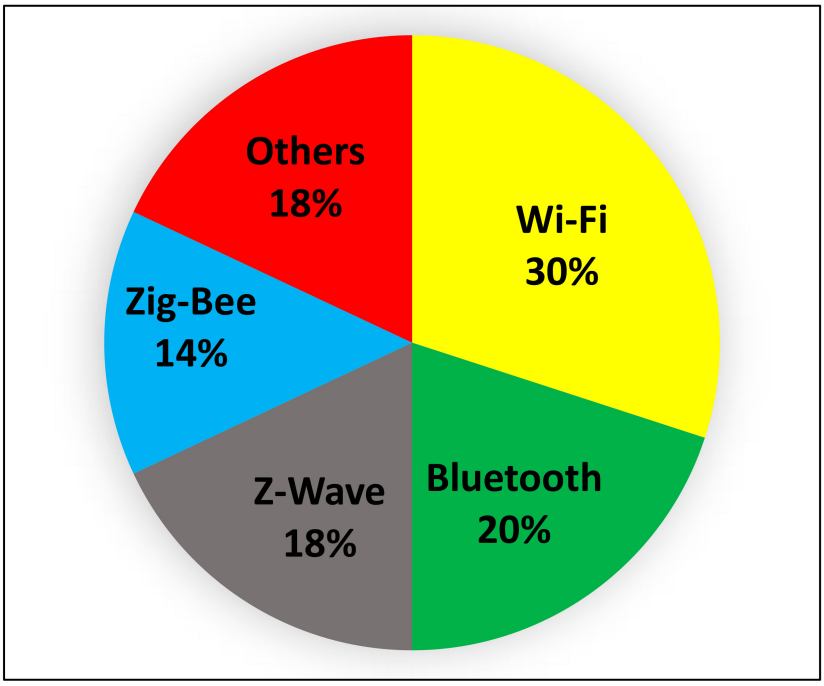

Figure 4. Statistics of the use of different protocols in smart home devices.

4. Home Automation System Based on Bluetooth

Bluetooth is a wireless communication module optimized to provide an alternative to cables and is used to exchange information over short distances [49,50]. A home automation system based on Bluetooth has high security and can be installed in homes at a minimum price. Also, with this protocol, users will be able to monitor and control the devices that are connected to the network [51,52]. This protocol, which uses 2400 to 2480 MHz frequencies, can provide a wireless connection up to a distance of 100 m and works with less certainty in some situations. In some environments, it is impossible to maintain this protocol's relationship. The coverage range of this protocol is less than other wireless communication protocols, such as Wi-Fi. In general, security and communication protocols are significant issues, and, unfortunately, in the case of Bluetooth, this security is not specific and can be hacked [53]. A home automation system based on Bluetooth consists of an electronic hardware part. Figure 5 shows that the smart building management system includes an Android phone and Bluetooth Arduino (BT) that communicate with each other through Bluetooth [54,55]. Another method is to use the HC-05 Bluetooth module, which has become very popular among users due to its low price, easy access, that it can be set up with an Arduino board, and that it works as an IEEE802.11 wireless module [56,57]. The module is powered by a standard 5 V power supply and is serially connected to the Arduino with just one tap on the mobile app. Also, another method, HC-06, can be used, which is connected to an Arduino board, with household appliances then connected to the Arduino board through the relay [58]. This method has solved the needs of users and is also useful for people who are old and have physical disabilities [56]. For example, Figure 5 shows a designed home automation system that any smartphone can control via Bluetooth. The smartphone sends control signals to turn home appliances on or off through a Bluetooth-based Android application. According to the studies conducted in the article [59], a solution has been created to solve the challenges in smart building management using Firebase and Bluetooth. Bluetooth supports both data and audio, which makes it a superior technology and which has enabled many devices to communicate [60,61].

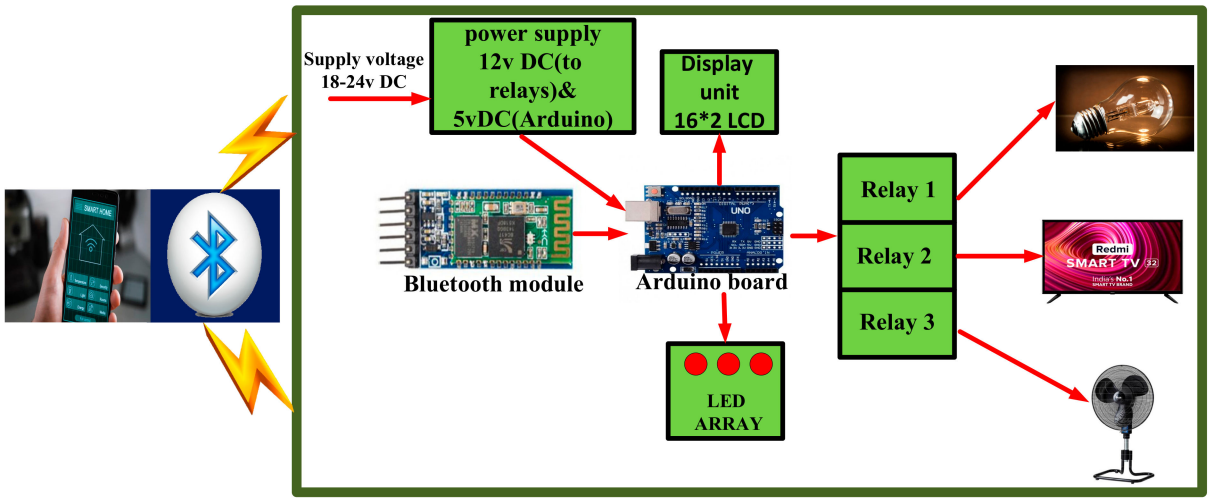

Figure 5. Bluetooth-based home automation system.

5. Home Automation System Based on Zig-Bee

Zig-Bee protocol is a wireless technology that works in three radio bands: 868 MHZ, 2.4 2 GHZ, and 915 MHZ [62]. The same data rate technology of 40–250 kbps and range of 1–100 m with the IEEE 802.15.4 standard was approved in December 2003, and Zig-Bee Alliance released the first version of this technology in 2006 [63]. In terms of IEEE standards, this protocol is very similar to Wi-Fi and Bluetooth standards [64]. Similar to Z-Wave, Zig-Bee is a mesh protocol. These devices can communicate with each other and will be able to act as repeaters [65]. After the production of the first product based on the Zig-Bee protocol, companies connected to this global technology. With its expansion, the Zig-Bee smart building standard entered the market. It connected thousands of devices wirelessly [66]. Zig-Bee Standard and Zig-Bee Smart Energy Parameter (SEP) have been identified by the National Institute for Protocols and Technology (NIST) [67,68] as the most appropriate communication standards for the smart grid home network area [69,70].

5.1. Constituents of Zig-Bee Network Function

Zig-Bee devices may come with all the capabilities of a Zig-Bee network, called a Full Function Device (FFD). Also, Zig-Bee devices may come with limited software capabilities called Reduced Function Devices (RFD) [71]. Based on the literature, an FFD device can communicate with all kinds of devices in a network. Therefore, these devices must be permanently active in the network. Unlike FFD devices, RFD devices can only connect with one FFD device. In most cases, it is intended to implement simple applications such as switching devices on and off. FFD and RFD devices in a network can be coordinators, PAN coordinators, or devices. PAN coordinators and coordinators fall under the category of FFD devices; however, the device may fall under the category of FFD or RFD devices. According to the literature, the coordinator is the most potent component of the FFD device that can send and receive messages. Also, the PAN coordinator is the central controller in a personal local area network. Now, if the device is not a coordinator, it can be called a device. According to the reference materials about FFD and RFD devices, the Zig-Bee standard makes three Zig-Bee protocol devices: Coordinator, Router, and End Device [72]. The Zig-Bee coordinator is a PAN coordinator in the IEEE 802.15.4 network and is responsible for establishing the network [73]. The Zig-Bee router is an FFD device that enables various Zig-Bee networks. By using a router, more devices can be added to the network. A router may also act as a Zig-Bee End device. Finally, the end devices are not routers and coordinators and are physically connected to a sensor or perform a control function that consumes less battery and can be FFD or RFD, depending on the application [73]. Figure 6 shows the layers related to the architecture of this protocol.

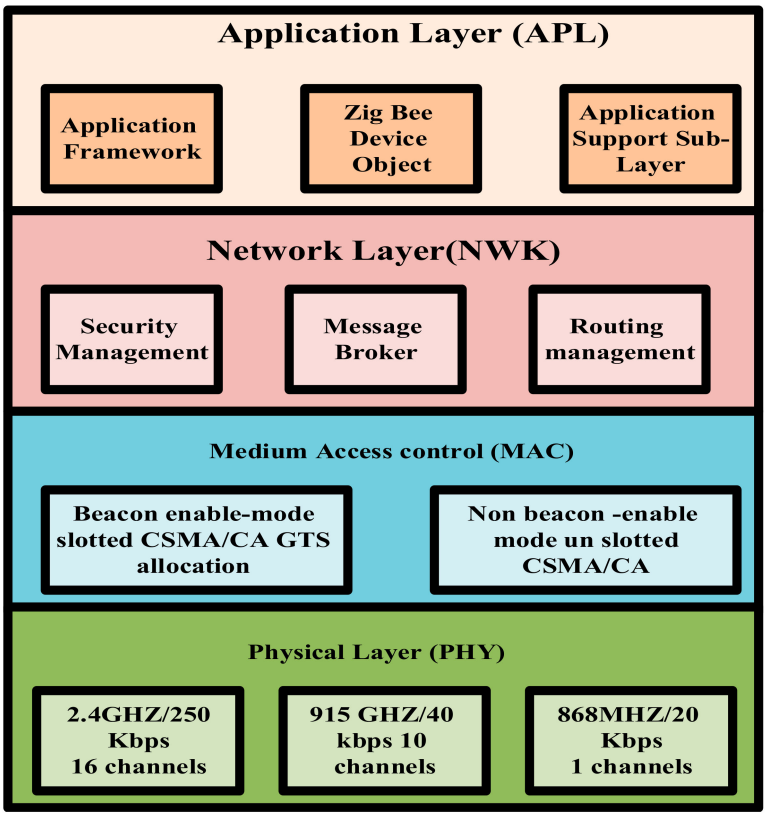

Figure 6. Architecture of Zig-Bee protocol.

5.2. The Architecture Related to Zig-Bee Protocol

The Zig-Bee protocol generally consists of four layers:

1. The first layer of the Zig-Bee protocol is called the Application Layer (APL). This layer converts input to digital data, change input to digital data, and digital data to output [74].
2. The next layer specifies the source and destination of the information. The logical transformation of addresses to be understandable for layering is done in this layer. Also, traffic network control is done in this layer. One of the most essential devices in computer networks, called the router, operates in this layer because, in this layer, information packets (Packets) deal with the IP protocol for the route, and the router works with IP [75].
3. (MAC): This layer employs the carrier sensed multiple access with collision avoidance (CSMA-CA) mechanism for channel access, personal area network (PAN) association, disassociation, network synchronization beacons, and device security [75].
4. (PHY): This layer includes radio communication (modulation and demodulation), which is responsible for transmission and reception. With a frequency of 2.4 GHz in this layer, information can be sent and received up to 250 kbps [74].

5.3. Topology

The EEE802.15.4 standard can support four types of topological networks with more than 64,000 nodes, two of them being star-tree-cluster-tree and star-mesh; however, Zig-Bee is only able to use tree topology [76,77]. Mesh topology, as a peer-to-peer network, consists of a coordinator and several routers and nodes. In this topology, it is easy to add or remove a device in the web, and if a problem occurs during data transmission in one path, the node finds another way and reaches the destination [78,79]. Also, in this topology, energy consumption is more optimal because the devices are close to each other. In a star topology, there is no router, although there is a coordinator and several end devices. One of the disadvantages of this topology is that, if the coordinator fails,

the entire network becomes inactive. Since there is no alternative path from the source to the destination, the coordinator suffers. Cluster tree topology is a particular case of tree topology in which parents, together with their children, are called a cluster. [80]. In a tree topology, the network consists of a central node that includes a coordinator, several routers, and nodes. According to Figure 7, this topology consists of several star networks. To form a tree topology, at least three hierarchical levels must be created: a coordinating device, a router, and an end device. Child end devices and coordinators are called producer routers. In general, a topology A tree is used in the construction of large networks, and the management and maintenance of computers are easily possible. In this topology, if the central device is damaged, the entire network will fail, which is one of the disadvantages of this topology.

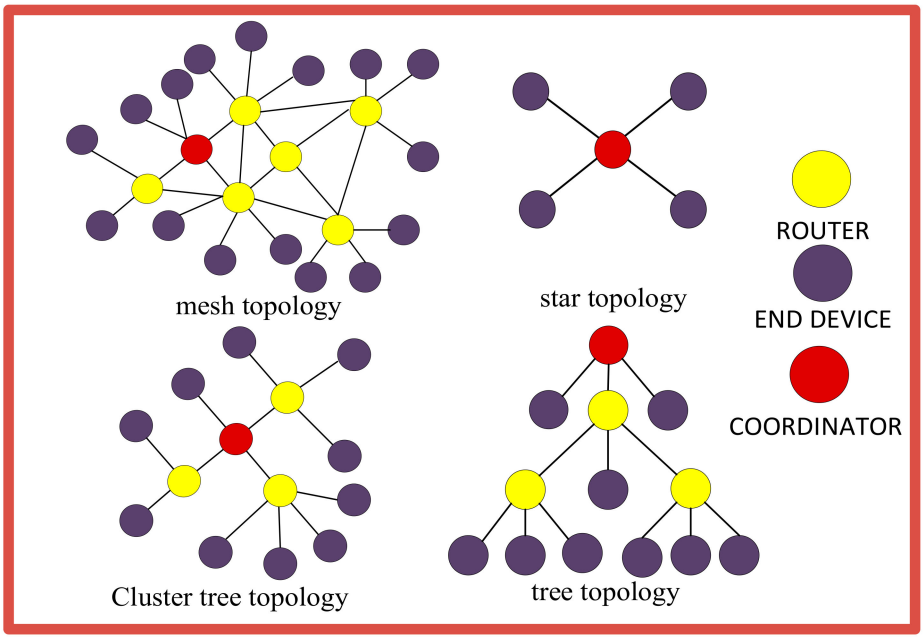

Figure 7. Topologies related to Zig-Bee protocol.

6. Home Automation System Based on Z-Wave

With the evolution of state-of-the-art applications and paradigms, the world is progressing toward smart cities. Smart homes are an important aspect of smart cities, wherein various mobile computing and network technologies are used. However, they are also susceptible to security threats that can cause serious issues related to privacy and safety. Z-Wave is a wireless technology that is primarily used in smart homes [81]. The Z-Wave protocol was started by the Danish company Zany's as a smart lighting control system for consumers and evolved into a home network automation mesh protocol implemented on a SOC-on-a-chip system [82]. This protocol was created in 2008 by Sigma designs company to replace other protocols, and it is now one of the most widely used protocols. Z-Wave technology is a technology of low-power radio waves developed to establish communication between household devices. Z-Wave was described as a new wireless home automation technology that uses low power and communicates at a frequency of 900 MHz and a range of about 30 m. Reference [83] describes how Z-Wave can work in a smart home system. Further studies have been conducted to implement Z-Wave in specific applications such as monitor systems [84] and lock systems [85]. In addition, some authors have also focused on the security features of Z-Wave [86,87]. Z-wave devices have higher security due to the identification of the user and are also compatible with devices of different brands and can communicate with them [88]. The Z-Wave network supports mesh network topology, and a primary controller and several sub-controllers are responsible for establishing secure communication between devices [89]. In such a network, devices can communicate with

each other through intermediate nodes and, in this way, communication barriers and blind spots are eliminated. Z-Wave technology consists of three layers: the radio layer, the network layer, and the software layer. These three layers are connected to lead to a robust and secure network [90]. Figure 8 shows the architecture of this protocol.

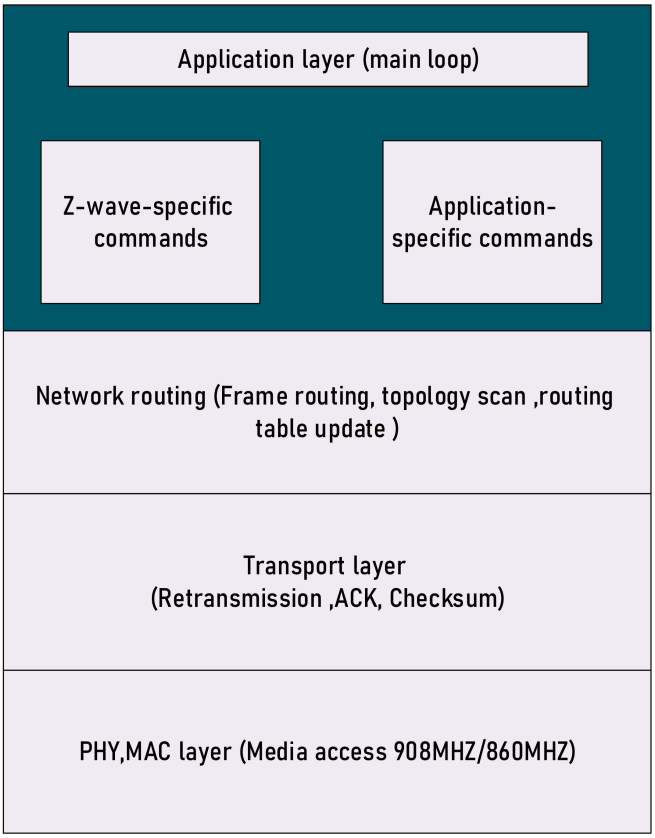

Figure 8. Architecture related to Z-wave protocol.

6.1. Radio Layer

In this layer, the path that the signal takes between the network and the hardware layer is defined. This layer includes frequency, encryption, and hardware access.

6.2. Network Layer

In the network layer, how to exchange data between devices or nodes is determined. The tasks of this layer include addressing, network organization, routing, etc.

6.3. Software Layer

In this layer, the messages and commands to be sent to other devices are defined. The network layer in Z-Wave technology includes three sub-layers for data transmission between different devices [91].

6.3.1. (MAC)

In this layer, the wireless communication hardware of the device is controlled. There is no access to this layer for the end user [92]. This is an anti-collision mechanism that ensures secure data transfer [93].

6.3.2. Transmission Layer

In this layer, the message transmission and wireless communication with another device are controlled. The end user does not have the possibility to change the performance of this layer, but he can see the results of its performance [94].

6.3.3. Routing Layer

Mesh network capability in Z-Wave is realized in this layer. The possibility of meshing in the network leads to an increase in the range of PAN networks. In this layer, the message reaches the destination device in the mesh network [92].

7. Home Automation System Based on Wi-Fi Protocol

The Wi-Fi protocol is a wireless communication protocol registered by the Wi-Fi Alliance and based on the IEEE 802.11 standard. This protocol provides a high data transfer rate of up to 1 GB depending on the 2.4 GHz channel and 5 GHz band within a range of 50 m [95,96]. The smart system based on the Wi-Fi protocol does not require a central controller, and the equipment communicates directly with the home modem. This protocol is mainly used for the wireless management of household appliances such as sockets [96,97]. Figure 9 shows a home automation system based on Wi-Fi technology. Figure 9 indicates that an Android mobile application with integrated Wi-Fi can easily control home appliances. Using this program, data can be transferred remotely using Wi-Fi technology. A preconfigured Wi-Fi device can be used to continuously update the status collected from the sensor on the firebase database [98]. This technology will remotely control service-specific convergence sublayer (SSCS) switches and devices using an Android app. Also, this technology has a more extended range than other protocols, and it can be possible to control several devices simultaneously from anywhere in the world. ESP826612E is used as a central controller and as a Wi-Fi chip in this case [99]. Transmission speed, high bandwidth, and availability are the advantages of this protocol. Most people use a Wi-Fi router in their home instead of Ethernet cables due to economic efficiency. Also, the Wi-Fi protocol is relatively safe and provides users access to the Internet anywhere in the house. However, in terms of home automation, in the Wi-Fi-based smart home, there are problems such as the problem of power consumption of Wi-Fi devices, range limitation in large houses, and interference in the network.

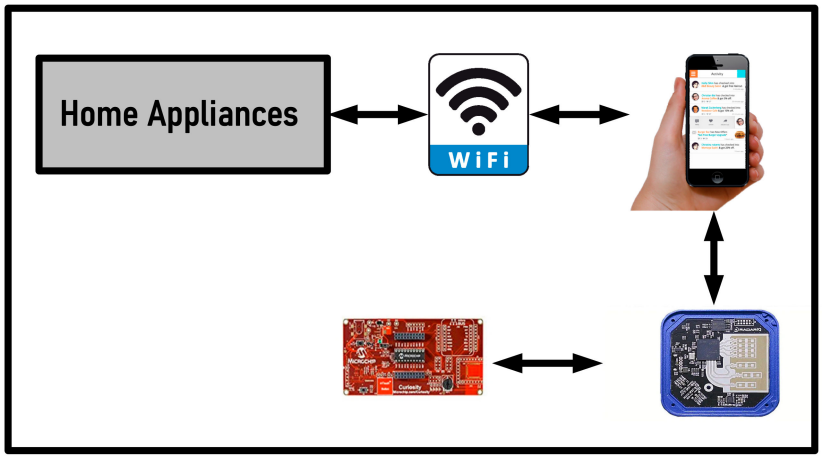

Figure 9. Home automation system based on Wi-Fi protocol.

8. Home Automation System Based on 5G

With the rapid growth of the IoT, 5G is the next generation of wireless communication that significantly increases the speed and responsiveness of wireless technologies [100]. This technology creates new possibilities for various applications such as agriculture, transportation, etc. This article discusses the connection of the device to the device of this technology [101]. Also, 5G technology, which uses the millimeter wave spectrum, includes:

- High-band waves (above 6 GHz);
- Medium-band waves (2 to 4.5 GHz);
- Low-band waves such as the fourth generation (below 3 GHz).

Also, one of the essential goals of this new technology is to maximize the data transfer rate up to 20 Gb/s [102,103]. Furthermore, 5G technology is critical to developing smart cities because 5G creates excellent opportunities for connected devices in buildings and cities to help track, monitor, and control energy. It allows buildings and cities to better manage their energy resources, save costs, and become more sustainable [104].

Review of 5G Network Architecture

Traditionally, physical network hardware components for the 5G Core Network, such as servers, switches, and storage, will be offloaded entirely to the cloud and orchestrated in a virtual environment through intelligent software tools. Figure 10 demonstrates how everyday consumer devices such as smartphones, smart sensors, or connected automobiles cannot connect directly to the 5G Core Network on their own. In order to reach the 5G Core Network, User Equipment must first connect through 5G-enabled equipment on the Radio Access Network (such as a cell tower or small cell array) that will route traffic to the network core and the internet.

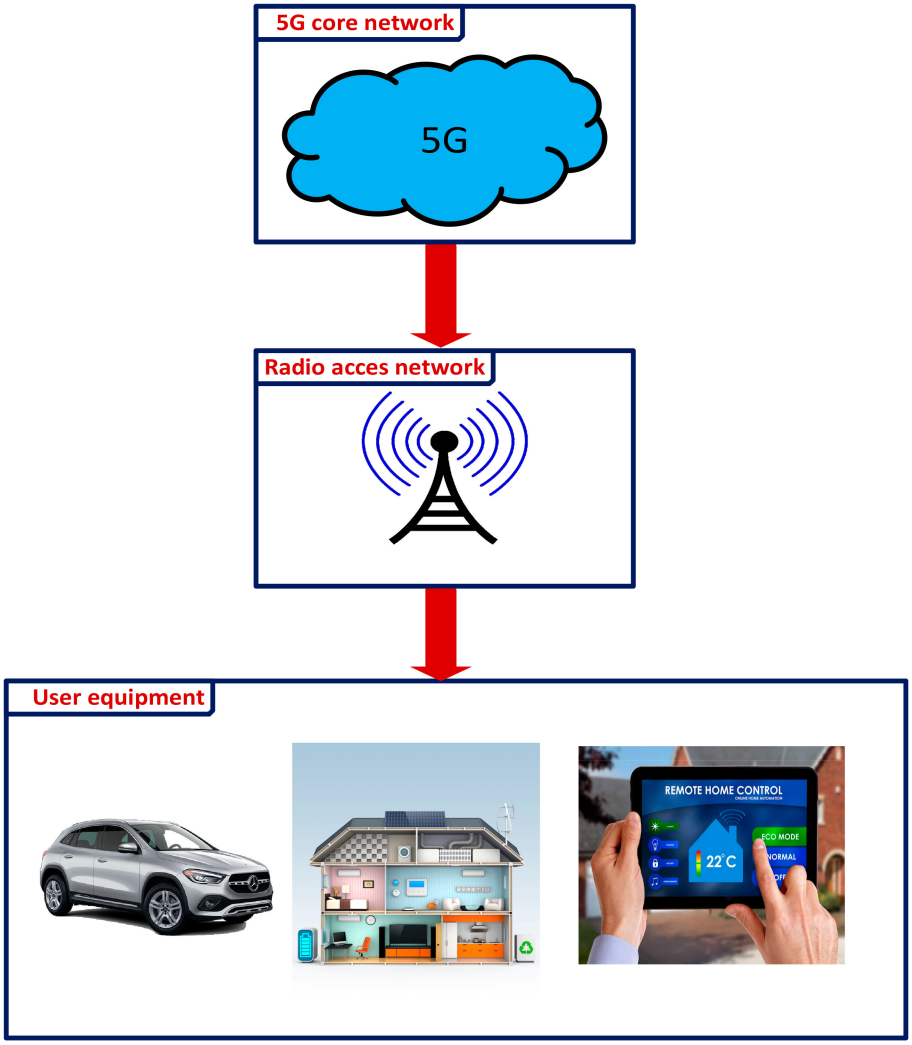

Figure 10. Overview of 5G network architecture.

9. Home Automation System Based on LoRaWAN

This protocol is a low-power, long-range LPWAN communication technology mainly designed to cover a vast area network in the IoT. This protocol has a data rate of from 0.3 to 50 kbps and a coverage range of from 2 to 5 km in the urban environment and 15 km outside the city [105]. This protocol works in Europe's 868 and 433 MHz bands, 915 MHz in America,

and 430 MHz in Asia. Also, equipment based on this protocol will work for a long time with one battery. The architecture of this protocol, as shown in Figure 11, includes sensors and operators called End-Device, gateways (LoRaWAN Gateways), network servers, and user applications and software. With this technology, information is collected by end devices or sensors and sent to gateways using the network. Then, those data will be sent to LoRaWAN servers utilizing gateways and the Internet and communication channels (LTE, 3G, Wi-Fi). Finally, after processing the information by the server, the required information will be sent to the users or Application Servers via the Internet LoRaWAN network topology type based on a star topology. Also, this technology consists of three different classes: A, B, and C. Class A devices support two-way communication between themselves and the Gateway. In addition to Class A, Class B devices synchronize with the network at scheduled times using periodic waves and downlink ping intervals. Through this method, the network can send downlink communications with unavoidable delay and increase the energy consumption of the end device. The delay time is programmable up to 128 s to vary with different applications, and the extra power consumption is low enough to still be reliable for applications that use the battery. In addition to the Class A structure that follows from the uplink, there are two downlink paths. Class C can hold the receiver of the end device and reduce the downlink latency when the device is not transmitting anything. Therefore, Class C is suitable for applications that require [106].

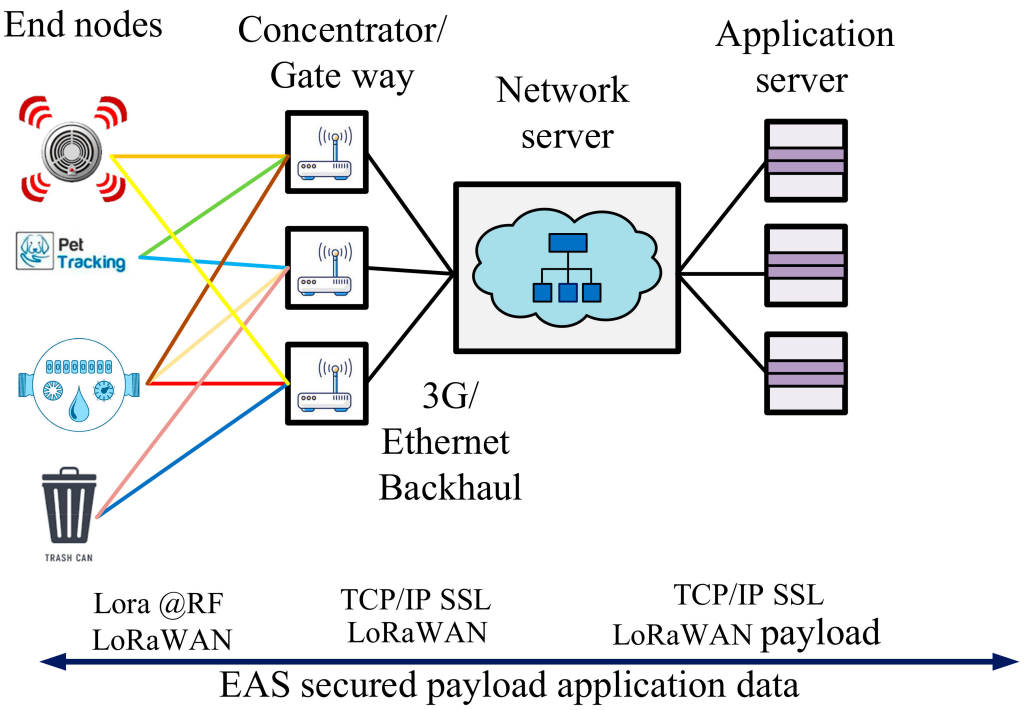

Figure 11. LoraWAN protocol architecture.

10. Home Automation System Based on 6LoWPAN

6LoWPAN combines the latest versions of the Internet Protocol (IPv6) and Low Power Wireless Personal Area Networks (LoWPAN), providing small devices with limited processing power to transmit information wirelessly. In general, this key communication technology is based on IP [102]. This problem was solved by **6LoWPAN** through adopting an intermediate network and communication layer in the IP stack and the ability to transmit IPv6 data packets through the IEEE 802.15.4 standard on radio transmission networks. For this reason, it changed the prevalent perspectives of the IoT [107]. The most important advantage of this protocol is the IPv6 stack, which recently played a prominent role in enabling IoT. The 6LoWPAN protocol provides about 5 × 1028 addresses for each user, which are assigned to each device separately, which allows the devices to connect to the

Internet with their IP address. This protocol was initially designed to support low-power networks with a frequency band of 2.4 GHZ, although, now, this technology is widely used in world.

10.1. 6LoWPAN Network Model

In this section, we will examine the nature of a 6LoWPAN protocol. This technology can support star and mesh topologies and 16-bit and IEE-EUI64-bit extended addresses [108]. Figure 12 shows the complete essence of this technology. As shown in the figure the 6LoWPAN gateway, located between two different networks, has the task of accurately implementing the matching layer function [109]. In the next part, the devices of this protocol, which are FFD and RFD, are examined. FFD devices can communicate with RFD devices and multiple FFD devices. These devices operate in three modes: a PAN coordinator, a coordinator, or an end device. RFD devices, unlike FFD devices, will only work as an end device, will only be able to communicate with an FFD, and are generally used for straightforward applications.

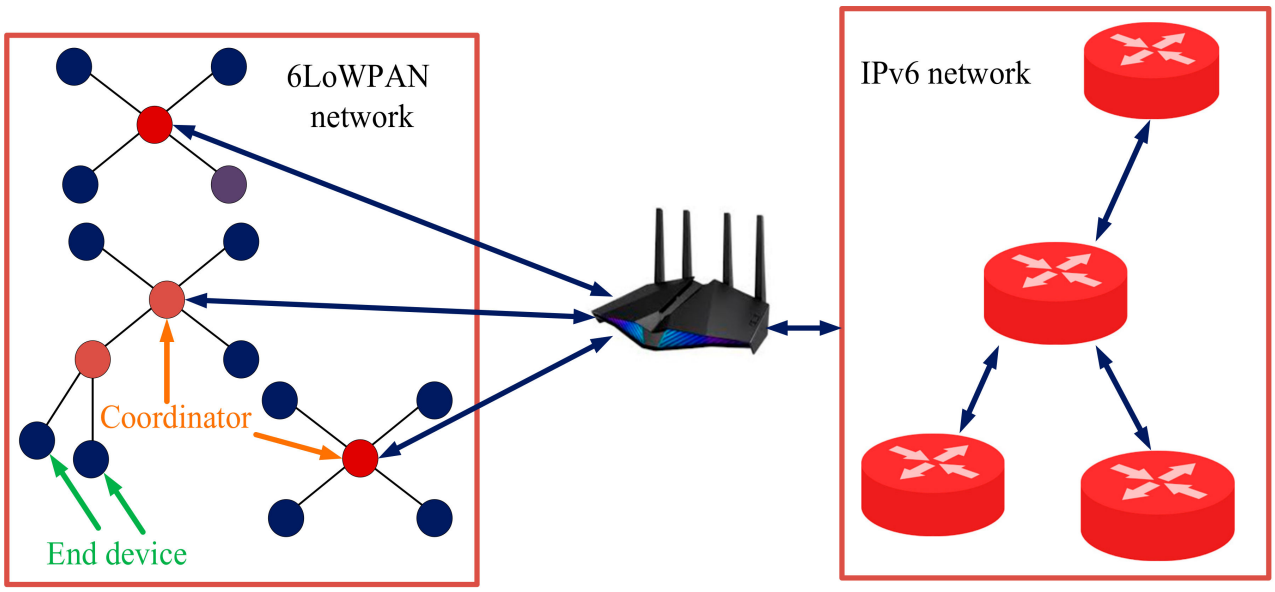

Figure 12. 6LoWPAN network model.

10.2. Review of the 6LoWPAN Protocol Stack

Figure 13 shows the 6LoWPAN protocol stack. According to the figure in Layers 1 and 2, MAC and PHY transmit the frames to the neighbors of the single hub. In Layer 3, it is necessary to fragment IPv6 packets and finally compress them; the reason for this problem is the limitation of 6LoWPAN protocol transmission (127 MTU). On Layer 4, 6LoWPAN neighbor discovery (6LoWPAN-ND) [110] disseminates context information for compressing arbitrary IPv6 network prefixes. Apart from this, 6LoWPAN-ND is a multi-hop version of IPv6 neighbor discovery and IPv6 stateless auto-configuration. Also, in Layer 4, the IPv6 Routing Protocol for Low-Power and lossy Networks (RPL) [111] routes IPv6 packets. On Layer 6, User Datagram Protocol (UDP)-based protocols, such as the Constrained Application Protocol (CoAP), are commonly employed.

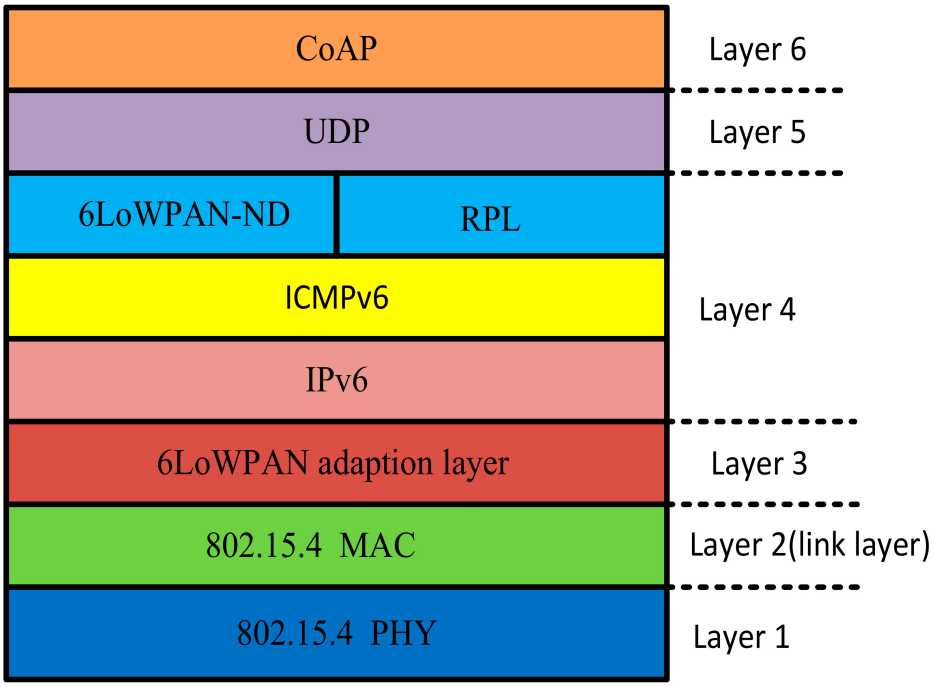

Figure 13. The 6LoWPAN protocol stack.

11. Privacy and Security

Security systems, in smart homes, means securing the house's entry points through sensors connected to a central controller. This controller is installed in one of the most accessible places in the house. These devices, which are directly or indirectly related to the Internet, create challenges for the security and privacy of smart home residents [112].

Data Privacy and Security in Smart Homes

In general, security in smart homes is related to data privacy and the safety of smart home residents. According to the research conducted by Mr. Zheng in reference [113], the safety of smart homes presents three critical issues:

1. Unauthorized entities are not allowed to access data. Therefore, impenetrability and decryption are essential in security issues related to smart homes;
2. Introducing entities that can access users' data and privacy;
3. Creating a safe environment for smart home users.

To protect users' privacy, symmetric and asymmetric essential encryption methods are usually used. The result of the encryption process is called cipher text. Also, the message that needs to be encrypted is called plaintext, which is converted into cipher text by a particular function called the key. The symmetric method uses data decoding, which is not the case in asymmetric. Also, all classical cryptography is symmetric, for example: DES, 3DES, and AES. Unlike symmetric encryption, in asymmetric encryption, a pair of public keys are used to encrypt and maintain confidentiality, and a private key is used for decryption. There is a mathematical relationship between them, for example, RSA, DH, and DSA [114]. In general, a smart home is vulnerable to two types of internal and external threats [115]. In both types of existing threats, hackers intend to compromise the smart home infrastructure [116,117]. Table 2 shows the threats and possible security damages in smart homes. As mentioned, all smart home systems work through home automation protocols. In addition, protocols are similar to languages through which smart home systems communicate with each other and execute commands. Table 3 describes the features and disadvantages of each of the protocols reviewed in this article.

Table 2. Threats, vulnerabilities and security issues related to protocols.

S.N.O.	Protocol Type	Examining Major Issues, Vulnerabilities and System Security
1	Bluetooth	• Blue jacking: Blue jacking typically involves hijacking another device's Bluetooth to send unsolicited messages, including business cards, advertisements, and pictures. Blue jacking usually happens within a 10-m range for smartphones or up to 100 m for laptops. • Blue bugging: Blue bugging is when the hacker uses a Bluetooth connection to install malware on the target device. This malware gives the hacker a backdoor to the target device, allowing them complete control of the device. For example, the attacker may be able to eavesdrop or initiate phone calls, access contact information, and read and send messages.
2	Zig-Bee	• Physical Attack: Zig-Bee network has a big weakness that all passwords are stored in memory without encryption. Therefore, if an intruder gains physical access to the device, he will be able to find the key by copying the information in the device's memory to the computer. (The location of the key is always in the same chip). • Therefore, to prevent this attack, all devices must be placed in a tamper-proof box, and if a violation is registered, the device must delete its memory [118]. • Key Attacks. • Replay Attacks: Secure networks always use trusted centers to keep their keys safe and multiple keys instead of one to protect against this attack [119].
3	Z-Wave	• Spoofing Attacks: Some of the challenges of spoofing attacks include the following: Transmission of false information in the IoT system, the vulnerability of IoT devices, endangering the decision-making process [120]. • Discover and create an external topology. • Arbitrary SR cache modification.
4	Wi-Fi	• WEP (Wired Equivalent privacy) and Wi-Fi protected access (WPA) can cracked in minutes. • WPA2 can also be cracked, only if user did not set it up properly.
5	LoraWAN	• Problem with gate compromise. • Physical device attack. • Problems with encryption keys. • Existence of non-optimal encryption methods.
6	5G	• This technology is vulnerable to information disclosure and spoofing attack. • Heavy network traffic. • Security issues of radio interfaces.
7	6LoWPAN	• Transport layer security constraints. • Security issues with datagram transport layer security.

Table 3. An overview of the advantages and disadvantages of communication protocols.

Protocol	Advantages	Disadvantages
Bluetooth	• Very high compatibility • Support for any device that can connect Bluetooth • reducing energy consumption	• Limited range Communication • Weak security • Pone to interference from IEEE 802.11 WLANs

Table 3. *Cont.*

Protocol	Advantages	Disadvantages
Zig-Bee	• Less energy consumption • High security • High connection speed • Low deployment cost • Low complexity • Support from many nodes • Easy monitoring	• This protocol will only be able to connect devices up to a distance of 60 feet, which is one of the disadvantages of this device • Interference the network • Difficult repair • High maintenance cost
Z-Wave	• Easy setup • The ability to connect devices to each other at distances of more than 550 feet • Low latency • Scalable	• Low audio and video quality • It is only able to connect 232 gadgets • Data transfer rate lower than Z-Wave
Wi-Fi	• Possibility of high productivity for subscribers • High reliability • The simplicity of this protocol due to the lack of additional hardware • Low price	• High energy consumption • It supports smaller distances • Weaknesses in some encryption methods
5G	• Low latency • High reliability • High speed • Ability to run a large number of device	• Security and privacy issues • Lack of technical support in most parts of world • Infrastructure development requires high cost
LoraWAN	• Low power • Long range • It does not interfere with other data rates • Two-way and secure	• It is not suitable for large data loads and the amount of the load is limited to 100 bytes • For continuous monitoring (except Class C devices).
6LoWPAN	• Robust • Low power support large mesh network topology • Can be applied across various communication platforms	• Require extensive training and knowledge • Short range • Low data rate

12. Challenges in Smart Homes and Future Trend

The studies conducted in references [121,122] present the challenges related to smart homes and provides solutions to solve these challenges. Reference [123] Does the same. In edge computing, deploying computing and storage resources is done at the location that produces the data. In the above architecture, computing and storage mechanisms are deployed right where the data source is located. Cloud computing refers to the massive and scalable deployment of computing and storage resources in different locations in other cities or even countries in terms of geographic location. Today, cloud computing is described as an alternative or sometimes a supplement to traditional data centers. In addition, cloud providers can prepare a set of pre-prepared services that can be used in various applications, such as the IoT, and provide them to consumers. Hence, the cloud is an efficient centralized platform for deploying the IoT. Even in a situation where cloud computing offers rich resources and services for complex analysis, the nearest cloud center may be hundreds of kilometers away from the point that generated the data. For this reason, it is necessary to rely on high-speed communication channels on the Internet to send data for cloud use. The cloud can bring centralized computing much closer to the data source. Still, edge computing is less efficient than is the cloud. Choosing an efficient architecture for computing and deploying storage is not limited to the cloud or the edge.

The cloud may be far from the source of data generation, and edge computing may have limited resources or it may not be physically possible to deploy those resources on-site. To solve the above problems, a concept called fog computing was invented. According to the studies conducted in the field of fog computing, it aims to optimize communication between smart homes and develop lightweight algorithms to process local data and reduce the number of transmissions that are needed between devices. Also, a large amount of produced data needs to be stored, integrated, and analyzed with high accuracy. Distributed data processing systems, NoSQL databases, and business intelligence platforms are some proposed solutions to this problem. The abovementioned problem has been shown to reduce the spread of smart homes. The results from the model proposed by Shin et al. show that older users are more willing to use a smart home than young users. From this study, a strategy to attract young consumers is needed to increase market demand. In general, users aim to maximize home security, increase energy efficiency, improve the performance of household appliances, and so on. Overall, with optimal home management, smart homes can replace the traditional home setup [124,125]. Studies conducted by researchers in connection with smart home technology refer to primary and vital issues such as technical and social disturbances, the need for families to get to know each other, incomplete training for learning, and the risk of energy intensification. In response to security issues related to smart homes, it can be concluded that security and privacy benefits can be obtained without high costs and with minimal energy consumption. Although sensors and other devices can help enable smart home technology, the operation of smart homes and the services provided to users are done by smart home automation platforms. Also, Xu et al. introduce flexible software to communicate between smart homes and users. This proposed platform's design basis is one that can integrate heterogeneous devices. Therefore, it paves the way for interoperability and standardization. Also, the advantages of this flexible platform include proper management and planning for daily tasks, complete monitoring of smart home performance, and location-based home automation [126].

13. Conclusions

Smart grids are on the verge of creating a new revolution in electrical energy systems. Wireless network technologies, along with a fully developed and exclusive architecture, provide users and hardware equipment with the ability to communicate with each other through data transmission through waves without using physical platforms such as wires and cables. Therefore, a suitable wireless technology must be implemented for reliable communication. In this article, various parameters, such as data rate, available bandwidth, number of channels, etc., which affect the field of application in the smart network, have been classified and analyzed. Therefore, in the interest of promoting safe, smart homes, among the various communication protocols available, in this article, Zig-Bee, Bluetooth, Wi-Fi and Z-wave, 6LoWPAN, **LoraWAN**, and 5G protocols have been reviewed and analyzed along with their advantages and disadvantages. In general, the main goal of this article is to study and research to improve the existing protocols and ensure users' security and privacy with appropriate security measures.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Azid, S.I.; Kumar, S. Analysis and Performance of a Low Cost SMS Based Home Security System. *Int. J. Smart Home* **2011**, *5*, 15–24.
2. Mahmud Rana, G.M.S.; Mamun Khan, A.A.; Hoque, M.N.; Mitul, A.F. Design and Implementation of a GSM Based Remote Home Security and Appliance Control System. In Proceedings of the 2013 2nd International Conference on Advances in Electrical Engineering (ICAEE), Dkaka, Bangladesh, 19–21 December 2013; pp. 291–295. [CrossRef]
3. Majdi, A.; Dwijendra, N.K.A.; Muda, I.; Chetthamrongchai, P.; Sivaraman, R.; Hammid, A.T. A smart building with integrated energy management: Steps toward the creation of a smart city. *Sustain. Energy Technol. Assess.* **2022**, *53*, 102663. [CrossRef]
4. Xu, Z.; Wang, R.; Yue, X.; Liu, T.; Chen, C.; Fang, S.-H. FaceME: Face-to-Machine Proximity Estimation Based on RSSI Difference for Mobile Industrial Human–Machine Interaction. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3547–3558. [CrossRef]
5. Wang, C.; Zhang, Z.; Abedinia, O.; Farkoush, S.G.; Damacharla, P.; Javaid, A.Y.; Gallimore, J.J.; Devabhaktuni, V.K. Common Metrics to Benchmark Human-Machine Teams (HMT): A Review. *IEEE Access* **2018**, *6*, 38637–38655.
6. Ziegler, S.; Nikoletsea, S.; Krco, S.; Rolim, J.; Fernandes, J. IoT and Crowd Sourcing—A Paradigm Change for the Research on the IoT. In Proceedings of the 2015 IEEE 2nd World Forum on IoT (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 395–399.
7. Hassan, Q.F. Introduction to the IoT. In *IoTA to Z: Technologies and Applications*; IEEE: Piscataway, NJ, USA, 2018.
8. Kotsiopoulos, T.; Sarigiannidis, P.; Ioannidis, D.; Tzovaras, D. Machine Learning and Deep Learning in Smart Manufacturing: The Smart Grid Paradigm. *Comput. Sci. Rev.* **2021**, *40*, 100341. [CrossRef]
9. Babar, M.; Khattak, A.S.; Jan, M.A.; Tariq, M.U. Energy Aware Smart City Management System Using Data Analytics and IoT. *Sustain. Energy Technol. Assess.* **2021**, *44*, 100992. [CrossRef]
10. Ben Atitallah, S.; Driss, M.; Boulila, W.; Ben Ghézala, H. Leveraging Deep Learning and IoT Big Data Analytics to Support the Smart Cities Development: Review and Future Directions. *Comput. Sci. Rev.* **2020**, *38*, 100303. [CrossRef]
11. Vermesan, O.; Friess, P.; Guillemin, P.; Gusmeroli, S.; Sundmaeker, H.; Bassi, A.; Jubert, I.S.; Mazura, M.; Harrison, M.; Eisenhauer, M.; et al. *Internet of Things Strategic Research Roadmap. InInternet of Things-Global Technological and Societal Trends from Smart Environments and Spaces to Green ICT*; River Publishers: Aalborg, Denmark, 2022; pp. 9–52.
12. Chaurasia, T.; Jain, P.K. Enhanced Smart Home Automation System based on Internet of Things. In Proceedings of the 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 12–14 December 2019; pp. 709–713. [CrossRef]
13. Jacobsson, A.; Boldt, M.; Carlsson, B. A risk analysis of a smart home automation system. *Future Gener. Comput. Syst.* **2016**, *56*, 719–733. [CrossRef]
14. Compton, M.; Barnaghi, P.; Bermudez, L.; García-Castro, R.; Corcho, O.; Cox, S.; Graybeal, J.; Hauswirth, M.; Henson, C.; Herzog, A.; et al. The SSN ontology of the W3C semantic sensor network incubator group. *J. Web Semant.* **2012**, *17*, 25–32. [CrossRef]
15. Collotta, M.; Pau, G. Bluetooth for Internet of Things: A fuzzy approach to improve power management in smart homes. *Comput. Electr. Eng.* **2015**, *44*, 137–152. [CrossRef]
16. Singh, S.; Singh, N. IoT (IoT): Security Challenges, Business Opportunities & Reference Architecture for E-Commerce. In Proceedings of the 2015 International Conference on Green Computing and IoT(ICGCIoT), Greater Noida, India, 8–10 October 2015; pp. 1577–1581.
17. Kunkun, P.; Xiangong, L. Reliability Evaluation of Coal Mine IoT. In Proceedings of the 2014 International Conference on Identification, Information and Knowledge in the Internet of Things, Beijing, China, 17–18 October 2014; pp. 301–302. [CrossRef]
18. Moysiadis, V.; Sarigiannidis, P.; Vitsas, V.; Khelifi, A. Smart Farming in Europe. *Comput. Sci. Rev.* **2021**, *39*, 100345. [CrossRef]
19. Sun, T.; Xu, Y.; Li, J.; Zhang, H. Research on IoTMiddleware Technology for Laboratory Environmental Monitoring. In Proceedings of the 2018 International Conference on Virtual Reality and Smart Systems (ICVRIS), Changsha, China, 10–11 August 2018; pp. 544–547.
20. Ahmad, K.; Maabreh, M.; Ghaly, M.; Khan, K.; Qadir, J.; Al-Fuqaha, A. Developing Future Human-Centered Smart Cities: Critical Analysis of Smart City Security, Data Management, and Ethical Challenges. *Comput. Sci. Rev.* **2022**, *43*, 100452. [CrossRef]
21. Perez, A.J.; Zeadally, S. Secure and Privacy-Preserving Crowdsensing Using Smart Contracts: Issues and Solutions. *Comput. Sci. Rev.* **2022**, *43*, 100450. [CrossRef]
22. Kung, Y.; Liou, S.; Qiu, G.; Zu, B.; Wang, Z.; Jong, G. Home Monitoring System Based IoT. In Proceedings of the 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 13–17 April 2018; pp. 325–327.
23. Bhatnagar, H.V.; Kumar, P.; Rawat, S.; Choudhury, T. Implementation Model of Wi-Fi Based Smart Home System. In Proceedings of the International Conference on Advances in Computing and Communication Engineering (ICACCE), Paris, France, 22–23 June 2018; pp. 23–28.
24. Demir, S.; Şimşek, Ş.; Gür, S.; Levi, A. Secure and Privacy Preserving IoT Gateway for Home Automation. *Comput. Electr. Eng.* **2022**, *102*, 108036. [CrossRef]
25. Lin, Y.-N.; Wang, S.-K.; Yang, C.-Y.; Shen, V.R.; Juang, T.T.-Y.; Hung, W.-H. Development and verification of a smart remote control system for home appliances. *Comput. Electr. Eng.* **2020**, *88*, 106889. [CrossRef]
26. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A Survey on Privacy and Security of IoT. *Comput. Sci. Rev.* **2020**, *38*, 100312. [CrossRef]
27. Schiller, E.; Aidoo, A.; Fuhrer, J.; Stahl, J.; Ziörjen, M.; Stiller, B. Landscape of IoT Security. *Comput. Sci. Rev.* **2022**, *44*, 100467. [CrossRef]

28. Jara, A.J. Wearable Internet: Powering Personal Devices with the IoTCapabilities. In Proceedings of the 2014 International Conference on Identification, Information and Knowledge in the IoT, Beijing, China, 17–18 October 2014; p. 7.
29. Domingo, M.C. An Overview of the IoTfor People with Disabilities. *J. Netw. Comput. Appl.* **2012**, *35*, 584–596. [CrossRef]
30. Gur, S.; Demir, S.; Simsek, S.; Levi, A. Secure and privacy-aware gateway for home automation systems. In Proceedings of the 13th International Conference on Security of Information and Networks, Istanbul, Turkey, 4–6 November 2020; pp. 1–10.
31. Vishwakarma, S.K.; Upadhyaya, P.; Kumari, B.; Mishra, A.K. Smart Energy Efficient Home Automation System Using IoT. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019. [CrossRef]
32. Ramlee, R.A.; Othman, M.A.; Leong, M.H.; Ismail, M.M.; Ranjit, S.S.S. Smart Home System Using Android Application. In Proceedings of the 2013 International Conference of Information and Communication Technology (ICoICT), Bandung, Indonesia, 20–22 March 2013; pp. 277–280.
33. Khunchai, S.; Thongchaisuratkrul, C. Development of Smart Home System Controlled by Android Application. In Proceedings of the 2019 6th International Conference on Technical Education (ICTechEd6), Bangkok, Thailand, 19–20 March 2019; pp. 1–4.
34. Sukandar, S.; Pongoh, D.S.; Ramschie, A.A.S. Design of Smart Home Control System Based on Android. In Proceedings of the 2018 International Conference on Applied Science and Technology (ICAST), Manado, Indonesia, 26–27 October 2018; pp. 165–170.
35. Standard, U.S. KNX Is the Standard. 2014. Available online: https://www.futurenergy.me/pdf/whatisknx.pdf (accessed on 4 November 2022).
36. KNX Specification, Version 1.1, Konnex Association, Diegem. 2004. Available online: https://www.auto.tuwien.ac.at/bib/pdf_thesis/THESIS0002.pdf (accessed on 4 November 2022).
37. Lázaro, J.; Abejón, S.; Astarloa, A.; Chamorro, F.; Bidarte, U. SoPC Implementation of the TP-KNX Protocol for Domotic Applications. In Proceedings of the 2008 International Conference on Advances in Electronics and Micro-Electronics, Valencia, Spain, 29 September–4 October 2008.
38. Oguntala, G.; Abd-Alhameed, R.; Jones, S.; Noras, J.; Patwary, M.; Rodriguez, J. Indoor Location Identification Technologies for Real-Time IoT-Based Applications: An Inclusive Survey. *Comput. Sci. Rev.* **2018**, *30*, 55–79. [CrossRef]
39. Khedr, A.M.; Aziz, A.; Osamy, W. Successors of PEGASIS Protocol: A Comprehensive Survey. *Comput. Sci. Rev.* **2021**, *39*, 100368. [CrossRef]
40. Kumar, T.; Mane, P.B. Zig-Bee Topology: A Survey. In Proceedings of the 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, India, 16–17 December 2016; pp. 164–166. [CrossRef]
41. Cheon, J.; Hwang, H.; Kim, D.; Jung, Y. IEEE 802.15. 4 ZigBee-based time-of-arrival estimation for wireless sensor networks. *Sensors* **2016**, *6*, 203. [CrossRef] [PubMed]
42. Samuel, S.S.I. A Review of Connectivity Challenges in IoT-Smart Home. In Proceedings of the 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 March 2016; pp. 1–4.
43. Danbatta, S.J.; Varol, A. Comparison of Zig-Bee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. In Proceedings of the 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 10–12 June 2019. [CrossRef]
44. Das, S.; Ganguly, S.; Ghosh, S.; Sarker, R.; Sengupta, D. A Bluetooth Based Sophisticated Home Automation System Using Smartphone. In Proceedings of the 2016 International Conference on Intelligent Control Power and Instrumentation (ICICPI), Kolkata, India, 21–23 October 2016; pp. 236–240.
45. Jakovljev, S.; Subotic, M.; Papp, I. Realisation of a Smart Plug Device Based on Wi-Fi Technology for Use in Home Automation Systems. In Proceedings of the 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 8–10 January 2017; pp. 327–328.
46. Fouladi, B.; Ghanoun, S. Security Evaluation of the Z-Wave Wireless Protocol. Available online: http://neominds.org/download/zwave_wp.pdf (accessed on 31 July 2017).
47. Pawar, P.N.; Ramachandran, S.; Singh, N.P.; Wagh, V.V.; Student, B.E. A Home Automation System Using the IoT. *Int. J. Innov. Res. Comput. Commun. Eng.* **2007**, 3297.
48. Rathnayaka, A.J.D.; Potdar, V.M.; Kuruppu, S.J. Evaluation of Wireless Home Automation Technologies. In Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), Daejeon, Korea, 31 May 2011–3 June 2011; pp. 76–81.
49. Sriskanthan, N.; Tandon, D.; Lee, K.K. Protocol for Plug and Play in Bluetooth Based Home Networks. *IEEE Trans. Consum. Electron.* **2004**, *50*, 457–462. [CrossRef]
50. Mulla, A.; Baviskar, J.; Khare, S.; Kazi, F. The Wireless Technologies for Smart Grid Communication: A Review. In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015; pp. 442–447. [CrossRef]
51. Marikyan, D.; Papagiannidis, S.; Alamanos, E. A systematic review of the smart home literature: A user perspective. *Technol. Forecast. Soc. Chang.* **2018**, *138*, 139–154. [CrossRef]
52. Palaniappan, S.; Hariharan, N.; Kesh, N.T.; Vidhyalakshimi, S.; AngelDeborah, S. Home Automation Systems—A Study. *Int. J. Comput. Appl.* **2015**, *116*, 11–18. [CrossRef]

53. Hassan, S.S.; Bibon, S.D.; Hossain, M.S.; Atiquzzaman, M. Security Threats in Bluetooth Technology. *Comput. Secur.* **2018**, *74*, 308–322. [CrossRef]
54. Ramlee, R.A.; Tang, D.H.; Ismail, M.M. Smart home system for disabled people via wireless bluetooth. In Proceedings of the 2012 International Conference on System Engineering and Technology (ICSET), Bandung, Indonesia, 11–12 September 2012; pp. 1–4.
55. Asadullah, M.; Ullah, K. Smart Home Automation System Using Bluetooth Technology. In Proceedings of the 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT), Karachi, Pakistan, 5–7 April 2017; pp. 1–6.
56. Shinde, A.; Kanade, S.; Jugale, N.; Gurav, A.; Vatti, R.A.; Patwardhan, M.M. Smart Home Automation System Using IR, Bluetooth, GSM and Android. In Proceedings of the 2017 Fourth International Conference on Image Information Processing (ICIIP), Shimla, India, 21–23 December 2017.
57. Yadav, R.K.; Vohra, H. Design Architecture and Comparison of Interactive Smart Button Using HC-05 and ESP8266. In Proceedings of the 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 5–6 May 2017; pp. 982–985. [CrossRef]
58. Kondaveeti, H.K.; Kumaravelu, N.K.; Vanambathina, S.D.; Mathe, S.E.; Vappangi, S. A systematic literature review on prototyping with Arduino: Applications, challenges, advantages, and limitations. *Comput. Sci. Rev.* **2021**, *40*, 100364. [CrossRef]
59. Debnath, B.; Dey, R.; Roy, S. Smart Switching System Using Bluetooth Technology. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019; pp. 760–763.
60. Porjazoski, M.; Latkoski, P.; Popovski, B. Bluetooth Low Energy-Based Smart Home Android Solution. In Proceedings of the IEEE EUROCON 2019-18th International Conference on Smart Technologies, Novi Sad, Serbia, 1–4 July 2019; pp. 1–5.
61. Adiono, T.; Anindya, S.F.; Fuada, S.; Afifah, K.; Purwanda, I.G. Efficient Android Software Development Using MIT App Inventor 2 for Bluetooth-Based Smart Home. *Wirel. Pers. Commun.* **2019**, *105*, 233–256. [CrossRef]
62. Types of Wireless Communication Technology Used in Home Automation. Available online: https://www.electronicsforu.com/technology-trends/learn-electronics/wireless-technology-types-home-automation (accessed on 4 November 2022).
63. Benakila, M.; George, L.; Femmam, S. A Beacon-Aware Device for the Interconnection of Zig Bee Networks. *IFAC Proc. Vol.* **2009**, *42*, 123–130. [CrossRef]
64. Olteanu, A.C.; Oprina, G.D.; Tapus, N.; Zeisberg, S. Enabling Mobile Devices for Home Automation Using Zig-Bee. In Proceedings of the 2013 19th International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 29–31 May 2013; pp. 189–195.
65. Batista, N.C.; Melicio, R.; Matias, J.C.O.; Catalao, J.P.S. Zig-Bee Wireless Area Network for Home Automation and Energy Management: Field Trials and Installation Approaches. In Proceedings of the 2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Berlin, Germany, 14–17 October 2012.
66. U.S. Department of Energy. 2011. Available online: https://www.energy.gov/sites/prod/files/DOE_CMS2011_FINAL_Full.pdf (accessed on 4 November 2022).
67. Nist Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. Smart Grid Cybersecurity Guidel. Interoperability Stand. (with DVD). 2012; pp. 19–133. Available online: https://www.nist.gov/system/files/documents/public_affairs/releases/smartgrid_interoperability_final.pdf (accessed on 4 November 2022).
68. Yi, P.; Iwayemi, A.; Zhou, C. Developing ZigBee Deployment Guideline Under WiFi Interference for Smart Grid Applications. *IEEE Trans. Smart Grid* **2010**, *2*, 110–120. [CrossRef]
69. Gungor, V.C.; Lu, B.; Hancke, G.P. Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Trans. Ind. Electron.* **2010**, *57*, 3557–3564. [CrossRef]
70. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [CrossRef]
71. Mihajlov, B.; Bogdanoski, M. Overview and Analysis of the Performances of Zig-Bee Based Wireless Sensor Networks. *Int. J. Comput. Appl.* **2011**, *29*, 28–35.
72. Shahzad, K.; Oelmann, B. A Comparative Study of In-Sensor Processing vs. Raw Data Transmission Using Zig-Bee, BLE and Wi-Fi for Data Intensive Monitoring Applications. In Proceedings of the 2014 11th International Symposium on Wireless Communications Systems (ISWCS), Barcelona, Spain, 26–29 August 2014; Volume 11, pp. 519–524.
73. Zig-Bee. Son Erişim: Nisan. 2019. Available online: https://acikerisim.dicle.edu.tr/xmlui/bitstream/handle/11468/4648/564065.pdf?sequence=1 (accessed on 4 November 2022).
74. Kaur, A.; Kaur, J.; Singh, G. Node Failure Investigation in Zig-Bee Sensor Network. *CT Int. J. Inf. Commun. Technol.* **2014**, *2*, 2321–7316.
75. Wang, J.; Chen, M.; Leung, V.C.M. Forming Priority Based and Energy Balanced Zig-Bee Networks—A Pricing Approach. *Telecommun. Syst.* **2013**, *52*, 1281–1292. [CrossRef]
76. Koç, Y. Akıllı Bir Takip Sistemi İçin Kullanılan Zig-Bee Tabanlı Algılayıcı Ağın Topolojik Performans Karşılaştırmaları. iErciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergis; Türkiye. 2013, Volume 31, pp. 165–171. Available online: https://dergipark.org.tr/tr/download/article-file/235975 (accessed on 4 November 2022).
77. Bhumika; Parmar, A.S. Performance Evaluation of Zig-Bee 802.15.4 WPAN in Logical Subnet in OPnet Modeler. In Proceedings of the 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, India, 19–20 March 2015. [CrossRef]

78. Wijetunge, S.; Gunawardana, U.; Liyanapathirana, R. IEEE 802.15.4 Based Hybrid MAC Protocol for Hybrid Monitoring WSNs. In Proceedings of the 38th Annual IEEE Conference on Local Computer Networks, Sydney, NSW, Australia, 21–24 October 2013.
79. Ocenasek, P. Towards security issues in ZigBee architecture. In *Symposium on Human Interface*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 587–593.
80. Mumtaz, M.; Al-Mukhtar, A.; Hadi, T.H. A Monitoring System Using Wireless Sensor Network. *J. Al-Nahrain Univ.* **2014**, *17*, 219–226.
81. Kim, K.; Cho, K.; Lim, J.; Jung, Y.H.; Sung, M.S.; Kim, S.B.; Kim, H.K. What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol. *Pervasive Mob. Comput.* **2020**, *66*, 101211. [CrossRef]
82. Yassein, M.B.; Mardini, W.; Khalil, A. Smart Homes Automation Using Z-Wave Protocol. In Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September 2016. [CrossRef]
83. Benhamaid, S.; Bouabdallah, A.; Lakhlef, H. Recent advances in energy management for Green-IoT: An up-to-date and comprehensive survey. *J. Netw. Comput. Appl.* **2022**, *198*, 103257. [CrossRef]
84. Gong, J.; Tan, C.; Liu, L.; Zhou, L. A New Monitoring System of Portable Microcomputer Injection Pumps Based on Z-Wave. In Proceedings of the 2016 Eighth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Macau, China, 11–12 March 2016; pp. 19–21.
85. Wei, C.C.; Chen, Y.M.; Chang, C.C.; Yu, C.H. The Implementation of Smart Electronic Locking System Based on Z-Wave and Internet. In Proceedings of the 2015 IEEE International Conference on Systems, Man, and Cybernetics, Hong Kong, China, 9–12 October 2015; pp. 2015–2017.
86. Badenhop, C.W.; Graham, S.R.; Ramsey, B.W.; Mullins, B.E.; Mailloux, L.O. The Z-Wave routing protocol and its security implications. *Comput. Secur.* **2017**, *68*, 112–129. [CrossRef]
87. Fuller, J.D.; Ramsey, B.W. Rogue Z-Wave Controllers: A Persistent Attack Channel. In Proceedings of the 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), Clearwater Beach, FL, USA, 26–29 October 2015; pp. 734–741.
88. Z-Wave Alliance Z-Wave Devices and Standards. 2017. Available online: https://www.sourcesecurity.com/news/co/z-wave-alliance.html (accessed on 4 November 2022).
89. Z-Wave. An Introductory Guide to Z-Wave Technology. 2013. Available online: https://digitalassets.resideo.com/damroot/Original/10010/Guide_Z-Wave.pdf (accessed on 4 November 2022).
90. Bihl, T.J.; Bauer, K.W.; Temple, M.A.; Ramsey, B. Dimensional reduction analysis for Physical Layer device fingerprints with application to ZigBee and Z-Wave devices. In Proceedings of the MILCOM 2015-2015 IEEE Military Communications Conference, Tampa, Florida, USA, 26–28 October 2015; pp. 360–365.
91. Varol, A.B. Compilation of Data Link Protocols: Bluetooth Low Energy (BLE), ZigBee and Z-Wave. In Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11–15 September 2019; pp. 85–90. Available online: https://www.semanticscholar.org/paper/Compilation-of-Data-Link-Protocols%3A-Bluetooth-Low-Varol/05624dda8a55b3e103e552110eb2cb2c4a63ad5a (accessed on 4 November 2022).
92. Z-Wave. Z-Wave Protocol Overview. v. 4, May 2007. Available online: https://www.wccandm.services/pdf/page_producten/ZWave/Z-Wave%20Protocol%20Overview.pdf (accessed on 4 November 2022).
93. Maitra, T.; Roy, S. A Comparative Study on Popular MAC Protocols for Mixed Wireless Sensor Networks: From Implementation Viewpoint. *Comput. Sci. Rev.* **2016**, *22*, 107–134. [CrossRef]
94. Yassein, M.B.; Mardini, W.; Almasri, T. Evaluation of security regarding Z-Wave wireless protocol. In Proceedings of the Fourth International Conference on Engineering & MIS 2018, Istanbul, Turkey, 19–20 June 2018; pp. 1–8.
95. Kumkar, V.; Tiwari, A.; Tiwari, P.; Gupta, A.; Shrawne, S. Vulnerabilities of Wireless Security Protocols (WEP and WPA2). *Int. J. Adv. Res. Comput. Eng. Technol.* **2012**, *1*, 34, ISSN 2278-1323.
96. Horyachyy, O. Comparison of Wireless Communication Technologies Used in a Smart Home: Analysis of Wireless Sensor Node Based on Arduino in Home Automation Scenario. 2017. Available online: https://www.semanticscholar.org/paper/Comparison-of-Wireless-Communication-Technologies-a-Horyachyy/95a428d471da60ee02f2423431c99bb6f440bad3 (accessed on 4 November 2022).
97. Gomez, C.; Paradells, J. Wireless home automation networks: A survey of architectures and technologies. *IEEE Commun. Mag.* **2010**, *48*, 92–101. [CrossRef]
98. Sivapriyan, R.; Rao, K.M.; Harijyothi, M. Literature Review of IoT based Home Automation System. In Proceedings of the 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 8–10 January 2020; pp. 101–105. [CrossRef]
99. Raju, K.; Lova, V.; Chandrani, S.K.; Begum, S.; Devi, M.P. Home Automation and Security System with Node MCU Using IoT. In Proceedings of the 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECo), Vellore, India, 30-31 March 2019.
100. Mendonça, S.; Damásio, B.; de Freitas, L.C.; Oliveira, L.; Cichy, M.; Nicita, A. The rise of 5G technologies and systems: A quantitative analysis of knowledge production. *Telecommun. Policy* **2022**, *46*, 102327. [CrossRef]
101. Pana, S.V.; Babalola, O.P.; Balyan, V. 5G Radio Access Networks: A Survey. *Array* **2022**, *14*, 100170. [CrossRef]
102. Moongilan, D. 5G Wireless Communications (60 GHz Band) for Smart Grid—An EMC Perspective. In Proceedings of the 2016 IEEE International Symposium on Electromagnetic Compatibility (EMC), Ottawa, ON, Canada, 25–29 July 2016.

103. Garau, M.; Anedda, M.; Desogus, C.; Ghiani, E.; Murroni, M.; Celli, G. A 5G Cellular Technology for Distributed Monitoring and Control in Smart Grid. In Proceedings of the 2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Cagliari, Italy, 7–9 June 2017; pp. 1–6.
104. Oughton, E.J.; Lehr, W.; Katsaros, K.; Selinis, I.; Bubley, D.; Kusuma, J. Revisiting Wireless Internet Connectivity: 5G vs. Wi-Fi 6. *Telecommun. Policy* **2021**, *45*, 102127. [CrossRef]
105. Saleem, Y.; Crespi, N.; Rehmani, M.H.; Copeland, R. IoT-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions. *IEEE Access* **2019**, *7*, 62962–63003. [CrossRef]
106. Reddy, G.P.; Kumar, Y.V.P.; Chakravarthi, M.K. Communication Technologies for Interoperable Smart Microgrids in Urban Energy Community: A Broad Review of the State of the Art, Challenges, and Research Perspectives. *Sensors* **2022**, *22*, 5881. [CrossRef]
107. Desogus, C.; Anedda, M.; Murroni, M.; Muntean, G.M. A traffic type-based differentiated reputation algorithm for radio resource allocation during multi-service content delivery in 5G heterogeneous scenarios. *IEEE Access* **2019**, *7*, 27720–27735. [CrossRef]
108. Montenegro, G.; Kushalnagar, N.; Hui, J.; Culler, D. Transmission of IPv6 Packets over IEEE 802.15. 4 Networks. No. Rfc4944. 2007. Available online: https://datatracker.ietf.org/doc/rfc4944/ (accessed on 4 November 2022).
109. Mukhtar, H.; Kang-Myo, K.; Chaudhry, S.A.; Akbar, A.H.; Ki-Hyung, K.; Yoo, S.W. LNMP-Management Architecture for IPv6 Based Low-Power Wireless Personal Area Networks (6LoWPAN). In Proceedings of the NOMS 2008—2008 IEEE Network Operations and Management Symposium, Salvador, Brazil, 7–11 April 2008; pp. 417–424. [CrossRef]
110. Shelby, Z.; Chakrabarti, S.; Nordmark, E.; Bormann, C. Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). 2012. Available online: https://www.rfc-editor.org/rfc/rfc6775.html (accessed on 4 November 2022).
111. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Alexander, R.; Vasseur, J.P.; et al. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. *Netw. Archit. Serv.* **2012**, *6550*, 1–157. [CrossRef]
112. 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]
113. Zheng, Y.-L.; Ding, X.-R.; Poon, C.C.Y.; Lo, B.P.L.; Zhang, H.; Zhou, X.-L.; Yang, G.-Z.; Zhao, N.; Zhang, Y.-T. Unobtrusive Sensing and Wearable Devices for Health Informatics. *IEEE Trans. Biomed. Eng.* **2014**, *61*, 1538–1554. [CrossRef] [PubMed]
114. Poon, C.; Zhang, Y.-T.; Bao, S.-D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Commun. Mag.* **2006**, *44*, 73–81. [CrossRef]
115. Alkatheiri, M.S.; Alqarni, M.A.; Chauhdary, S.H. Cyber security framework for smart home energy management systems. *Sustain. Energy Technol. Assess.* **2021**, *46*, 101232. [CrossRef]
116. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-Fovino, I.; Steri, G.; Baldini, G. Security and Privacy Issues for an IoT Based Smart Home. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017.
117. Lee, C.; Zappaterra, L.; Choi, K.; Choi, H.-A. Securing Smart Home: Technologies, Security Challenges, and Security Requirements. In Proceedings of the 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 67–72. [CrossRef]
118. Snehi, M.; Bhandari, A. Vulnerability Retrospection of Security Solutions for Software-Defined Cyber–Physical System against DDoS and IoT-DDoS Attacks. *Comput. Sci. Rev.* **2021**, *40*, 100371. [CrossRef]
119. Ďurech, J.; Franeková, M. Security Attacks to Zig-Bee Technology and Their Practical Realization. In Proceedings of the 2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI), Herl'any, Slovakia, 23–25 January 2014.
120. Khan, F.; Al-Atawi, A.A.; Alomari, A.; Alsirhani, A.; Alshahrani, M.M.; Khan, J.; Lee, Y. Development of a Model for Spoofing Attacks in IoT. *Mathematics* **2022**, *10*, 3686. [CrossRef]
121. Stojkoska, R.; Trivodaliev, K.V. A Review of IoTfor Smart Home: Challenges and Solutions. *J. Clean. Prod.* **2017**, *140*, 1454. [CrossRef]
122. Wang, W.; Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
123. Shukla, A.; Katt, B.; Nweke, L.O.; Yeng, P.K.; Weldehawaryat, G.K. System Security Assurance: A Systematic Literature Review. *Comput. Sci. Rev.* **2022**, *45*, 100496. [CrossRef]
124. Shin, J.; Park, Y.; Lee, D. Who Will Be Smart Home Users? An Analysis of Adoption and Diffusion of Smart Homes. *Technol. Forecast. Soc. Change* **2018**, *134*, 246–253. [CrossRef]
125. Hargreaves, C.; Wilson, R. Hauxwell-Baldwin, Learning to Live in a Smart Home. *Build. Res. Inf.* **2018**, *46*, 127–139. [CrossRef]
126. Xu, K.; Wang, X.; Wei, W.; Song, H.; Mao, B. Toward software defined smart home. *IEEE Commun. Mag.* **2016**, *54*, 116–122. [CrossRef]