computers

Review

Generic IoT for Smart Buildings and Field-Level Automation—Challenges, Threats, Approaches, and Solutions

Andrzej Ożadowicz

Department of Power Electronics and Energy Control Systems, Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering, AGH University of Krakow, al. Mickiewicza 30, 30-059 Krakow, Poland; ozadow@agh.edu.pl; Tel.: +48-12-617-50-11

Abstract: Smart home and building systems are popular solutions that support maintaining comfort and safety and improve energy efficiency in buildings. However, dynamically developing distributed network technologies, in particular the Internet of Things (IoT), are increasingly entering the above-mentioned application areas of building automation, offering new functional possibilities. The result of these processes is the emergence of many different solutions that combine field-level and information and communications technology (ICT) networks in various configurations and architectures. New paradigms are also emerging, such as edge and fog computing, providing support for local monitoring and control networks in the implementation of advanced functions and algorithms, including machine learning and artificial intelligence mechanisms. This paper collects state-of-the-art information in these areas, providing a systematic review of the literature and case studies with an analysis of selected development trends. The author systematized this information in the context of the potential development of building automation systems. Based on the conclusions of this analysis and discussion, a framework for the development of the Generic IoT paradigm in smart home and building applications has been proposed, along with a strengths, weaknesses, opportunities, and threats (SWOT) analysis of its usability. Future works are proposed as well.

Keywords: building automation; Internet of Things; generic IoT; fieldbus; edge computing; fog computing; blockchain; machine learning; artificial intelligence; IoT assessment

Citation: Ożadowicz, A. Generic IoT for Smart Buildings and Field-Level Automation—Challenges, Threats, Approaches, and Solutions. *Computers* **2024**, *13*, 45. https://doi.org/10.3390/computers13020045

Academic Editor: Sergio Correia

Received: 22 December 2023
Revised: 21 January 2024
Accepted: 30 January 2024
Published: 3 February 2024

1. Introduction

The rapid development of Internet-of-Things (IoT) technology over the last dozen or so years has contributed to a significant increase in the diversity and heterogeneity of data-transmission networks, as well as the emergence of numerous standards, communication protocols, and approaches in network organization. However, technological progress and development in this area are inevitable, and the IoT paradigm is constantly gaining new application areas, in particular in the field of smart solutions, both industrial, commercial, and utility, dedicated directly to customers [1,2]. This diversity of applications generates the need to consider the various requirements and expectations of users and applications. For example, the implementation of IoT devices (smart nodes) in the control and monitoring network of a production line with industrial robots poses completely different challenges to network installers and integrators than in the case of identifying products and a purchasing application based on smart IoT labels or operating IoT modules with a smartphone in smart-home or smart-city installations [2–4]. Therefore, it is a difficult task to define and sanction a uniform universal generic IoT framework for all its potential application areas, although many research and engineering teams are making efforts. This paper focuses on the applications of smart-home technologies and smart-building systems, considering their inclusion in larger system structures such as local energy microgrids and smart cities [5–7].

1.1. Fieldbus Networks in Smart Homes and Buildings

Over the last thirty years, network-communication technologies and protocols for building and industrial automation systems, as well as information and communications technology (ICT) networks, have been developing independently of each other. In particular, to support various sensor and actuator modules characteristic for building automation and control systems (BACS) and building management systems (BMS) dedicated communication technologies have been developed to transmit short data packets in channels with relatively low bandwidth that are sufficient for this type of use. Physically, communication was and is implemented in most such systems through data buses with various types of communication media, most often a twisted pair and less often a power line, optical fiber, or radio channels. Three open, international standards, namely KNX [8], LonWorks [9], and BACnet [10], have been developed for BACS, dedicated to the implementation of fieldbus networks in buildings [11–14]. In addition, many manufacturers of building automation modules have developed and introduced their own, proprietary communication protocols, reserved to support the modules and devices they offer. Most of them are based on the seven-layer open systems interconnection model from the International Organization for Standardization (ISO/OSI model) providing a common basis for the purpose of systems interconnection [15–17]. Based on these technologies and protocols, distributed automation networks are built, operating in the event-based regime [18–21].

In turn, over the last ten to fifteen years, distributed systems with wireless communication of various technologies (Bluetooth, ZigBee, Z-Wave, and Wi-Fi) have become increasingly popular in the smart-home and smart-building market, especially for solutions dedicated to commercial and individual customers. In most cases, the organizational concept of such networks is based on a simplified configuration of network devices and control functions, using a smartphone, mobile devices, or Web services [22–26]. However, it should be noted that this integration in the physical and communication layer is mostly based on wireless Wi-Fi channels and the TCP/IP protocol. This is primarily due to the rapid increase in the popularity of Wi-Fi access points in private, public, commercial, and industrial buildings as an element of ensuring continuous, mobile, and remote communication with the buildings' infrastructure as well as their users/occupants. Moreover, people have used to almost constant use of smartphones and applications dedicated to them, including smart-home control and monitoring with Wi-Fi communication.

The mentioned wireless-communication technologies, such as Bluetooth Low Energy (BLE), ZigBee, or Z-Wave, tend to be used locally at the field level in home and building automation systems. This is mainly due to their short signal range and low power consumption. Therefore, they are implemented in various types of sensors (local measurement of temperature, pressure, CO_2 concentration, or light intensity) [26–31] and modules for location, user-activity tracking (beacons), and presence verification. In these applications, their short-range characteristics increase the precision of operation and can support the implementation of some building automation functions related to thermal comfort, adaptive control of heating, ventilation, and air conditioning (HVAC) systems, or dynamic regulation of room lighting [32–37]. Therefore, in relation to the generic IoT concept, they should only be considered as supporting technologies that cooperate with active nodes of KNX, LonWorks, BACnet, and ICT networks with TCP/IP protocol dedicated to IoT solutions.

These trends have opened the way to the expansion of IoT concepts and technologies as a solution not only for remote access to distributed BACS and BMS networks but also for communicating distributed modules with the TCP/IP protocol interface within such systems, at the field level as well. At the same time, however, the prospect of integrating ICT network technologies with fieldbus network technologies created the need to solve several technological and application problems [3,5,13,19,23,38,39]:

- Field-level IP protocol implementation with real-time requirements;

- Development of IoT structures for fieldbus networks;
- Assumptions for implementation of edge and fog services;
- Big-data processing within the edge and cloud computing for BACS and BMS;
- Cybersecurity and data privacy;
- Energy efficiency and energy consumption reduction for wireless modules, sensors, and actuators.

1.2. Edge and Fog Computing within Advanced Home and Building Automation Systems

The network and functional structures of modern BACS are characterized by the two most important features: (i) distribution—the possibility of installing universal microcontrollers performing simple control, monitoring, and communication functions directly in network nodes at the field level and (ii) integration—striving for mutual connection in one exchange network data control and monitoring functions for as many devices and building infrastructure subsystems as possible. Advances in digital technologies, as well as embedded systems based on System-on-a-Chip (SoC) architectures, have enabled the development of many control and monitoring devices (network nodes) that are powerful for support control and data communication functions directly at the field level, near the building infrastructure (for example, temperature and occupancy sensors, various actuators, such as valves, motors, etc.) [3,5,40]. In previous and some of the existing solutions, most of the functions of control modules, along with the data exchange between them, were implemented at the field level. However, with this approach, the desire to include an increasing number of new building infrastructure elements and devices in the network resulted in an increase in the resource load of these modules (memory, processor) and the use of communication bus bandwidth. Moreover, the prospect of developing BACS and BMS with the functions of dynamic response to changes in parameters and decision making in the implementation of energy-efficiency improvement mechanisms and transactive energy (for example, demand side management—DSM and demand side response—DSR) requires maintaining high time determinism and working in real-time mode (with minimal, deterministic data communication delays) [41–44].

To improve the responsiveness and correctness of the BACS and BMS, edge intelligence and devices have been proposed. They push processing for data-intensive, advanced control and monitoring functions away from the field-level nodes to a new edge network level, effectively handle local workloads, and make faster, more precise service decisions. Therefore, in the concept of smart home and smart building, one of the solutions turned out to be the expansion of BACS and BMS network structures with new SoC edge modules. They communicate with field-level nodes to collect data from sensors or provide signals to actuators, and, at the same time, they are responsible for handling higher-level data communication and local processing of advanced algorithms for monitoring, data acquisition, and control functions. Moreover, these edge modules, thanks to routing support and the inclusion in the TCP/IP network, also allow communication of smart-home and smart-building modules with external cloud services (databases, data analytics and visualization, cooperation with machine learning—ML, artificial intelligence—AI tools, and advanced algorithms). In this way, the IoT potential increases and introduces other development possibilities for BACS and BMS. Since the IoT edge nodes can increase computation near the source of the data, various IoT and cloud services can be deployed on local systems. This paradigm is known as ‘edge computing’ and integrates IoT technologies and cloud computing systems [45,46]. What is very important in smart home and building applications is that it reduces the communication bandwidth needed between sensors, actuators, and the external data center. Moreover, it allows for easier integration of different subsystems (energy, climate control, security, comfort, user services, maintenance, and energy management) controlled and monitored in modern, fully integrated intelligent facilities [3,39,47]. Therefore, this is one of the most important elements that should be included in the concept of a generic IoT framework for smart-building solutions.

A natural consequence of including edge modules from the IoT in BACS network structures, along with the computing and memory resources available in them (edge computing), is the emergence of a larger data exchange and processing structure called fog computing [45,46]. In [5], Taghizad-Tavana et al. explain that fog computing aims to optimize data transfer and communication between smart-building zones and smart homes and to develop lightweight algorithms to process local data and reduce the number of transmissions that are needed between devices. Moreover, according to [48,49] the fog computing paradigm is an alternative to smart modules with limited computational resources, typical for smart home and building systems. The authors explain that it extends the computational resources available in the cloud services to the network edge level, providing mobility, scalability, low latency, and robustness for the end BACS and BMS users. Additionally, what is very important is that edge computing enables real-time information analyses through the distribution of the decision-making process directly in the edge-level network at facilities (buildings, homes, local microgrids, etc.) [45]. Finally, Nasir et al. [39] add and explain that fog computing principally extends the cloud-computing architecture to the edge-level network. This approach enables an innovative variety of silent services and applications for end-users. Lightweight algorithms running on the edge-level network directly on IoT devices can conserve less bandwidth and provide computed, analyzed data to the end user without using the cloud every time. Moreover, the edge/fog modules can be equipped with AI mechanisms, providing more advanced computing and analyzing data in real time, thereby reducing the cloud service need and bandwidth. This approach and its features are very important considering the perspective of the development of advanced, dynamic control and monitoring functions for tactile internet, transactive energy management, generic IoT–fog–cloud BACS and BMS architectures as well as smart communities and cities [5,6,50,51].

1.3. Methodology of the Review

The wealth of conceptual and technical issues associated with the development of modern distributed smart home and building automation systems prompted the author to conduct a comprehensive review of the scientific literature of the last dozen years, particularly on the topic of integrating ICT networks and TCP/IP protocol transmission channels into these systems. The review is based on publication databases recognized in the electrical engineering, electronics, information technology and network control systems industry, namely ScienceDirect, Springer, IEEE Xplore, MDPI, and, occasionally, ACM Digital Library, Taylor and Francis, and Wiley Online Library. Moreover, in the selection of the main topics of the review, the results of analyses of the citations of publications in the Web of Science and Scopus databases and the population of selected keywords in patent databases (Google Patents search engine) were used.

Keywords were an important element in the guide to the literature review and in selecting specific publications for further discussion in this paper. They were divided into several thematic groups: (i) distributed control systems (e.g., building automation, fieldbus, smart home, smart building, BACS, and BMS); (ii) Internet of Things (e.g., smart nodes, edge computing, fog computing, cloud computing, TCP/IP for smart applications, and IoT maturity); (iii) communication networks (e.g., wired and wireless communication, remote access, local communication, and communication protocols); (iv) cybersecurity (e.g., privacy, data security, blockchain, access control, and encryption), and emerging trends (e.g., machine learning, artificial intelligence, tactile internet, and digital twin).

In many cases, combinations of several keywords led to the finding of other review texts, particularly those relating to IoT technologies and the areas of smart home and building applications. By analyzing these texts, the author identified potential thematic gaps and, based on them, formulated original contributions for this publication.

1.4. Original Contributions and the Paper Structure

According to the information presented in the previous subsections, IoT technologies have a very wide scope of applications. This review focuses on the specific smart home and building systems industries, considering the functionalities of advanced BACS and BMS. Moreover, several technical aspects of interactive energy management with DSM and DSR functions are discussed for smart home and building operations within local microgrids and smart-city infrastructures. In particular, the literature, research results, and case studies are analyzed in the context of developing the generic IoT concept for building automation systems in the framework of fieldbus–edge–fog–cloud architecture. The main contributions of this review are as follows.

- It provides a comprehensive review of the state-of-the-art IoT techniques and solutions related to smart homes and buildings with distributed control systems. This review is important because it collects knowledge about adapting and using IoT technologies in a segment that is rapidly developing but has so far been based on its own solutions for communication and data processing, in particular at the field level;
- As opposed to other IoT technology reviews, this one analyzes and discusses the suitability of various IoT concepts and tools for smart homes and buildings. Moreover, it sheds light on trends and innovative solutions emerging from this field that could be motivating for interested researchers and engineers;
- Providing a new perspective on various IoT applications (e.g., edge and fog computing and big-data processing) supported by recent research studies. To this end, the review provides some of the IoT design practices, considering the unique properties of smart homes and buildings, that finally will lead to more effective data processing, control and monitoring functions execution and better integration;
- It presents the major challenges and trends and pinpoints new, open research issues that need attention from researchers, domain experts, and engineers. In particular, this review provides information on the future scope of research on the integration of AI and ML capabilities, tactile internet developments, and IoT technology maturity assessment in building applications;
- It proposes general assumptions for the generic IoT framework concept with SWOT analysis as well as a discussion of pros and cons.

The remaining sections of this article are organized as follows. Section 2 presents a general view of network solutions, in particular distributed networks, used in home and building automation. Then, Section 3 describes the technological issues and main challenges related to the implementation of emerging edge and fog computing in BACS, BMS, and smart home and building systems. Section 4 selects and discusses several important trends and concepts for the development of functionally advanced BACS and BMS platforms with IoT technologies, in particular aspects of the implementation of ML and AI techniques. Section 5 introduces the generic IoT framework proposed by the author for applications in home and building automation systems, along with a SWOT analysis of its usability. Finally, in Section 6, the paper is concluded, providing future work information as well.

2. Control Networks and Smart Technologies in Buildings

In the classic engineering approach, technical solutions of smart home and building systems are based essentially on two organizational structures, (i) centralized systems, with one programmable logic controller (PLC) or server unit, cooperating with external modules supporting sensors and/or actuator modules and (ii) distributed systems, without a central unit but with sensor and actuator modules equipped with microcontrollers and communication interfaces. The second approach enables the execution of control and monitoring functions directly next to the elements of the house or building infrastructure, as well as data transfer between such modules, to implement more advanced functions within an integrated structure [52,53]. It should be noted that distributed solutions are the result of technological progress, development, and miniaturization of electronics, and they represent a significant achievement over the last several dozen years, enabling the implementation of more universal, advanced, and reliable system structures in the industrial and building automation industry. Obviously, centralized systems are still available and implemented in practice, but usually in very small installations (e.g., control of heating, ventilation, and air-conditioning systems in houses and small buildings), where they work well and are attractively priced. However, distributed systems are also becoming more and more popular in this sector. They are usually based on simple SoC modules with radio communication (Wi-Fi, Bluetooth, Z-Wave, ZigBee, and others), with dedicated applications for mobile devices or with support from dedicated server applications and websites [2,23,26,54,55]. Therefore, this study focuses on the analysis of the development of distributed automation networks, the architecture of which naturally fits into the concept of IoT technology applications and the cloud, with distributed tools and services for data processing.

2.1. Distributed Control Approach

The idea of distributed control systems in industrial and building automation developed in the 1990s and was a direct result of the appearance of microcontrollers that had sufficient computing power and memory resources to implement algorithms for the control and monitoring functions of industrial and building infrastructure devices. First, modules of various types of sensors and actuators were developed and equipped with microcontrollers and communication interfaces, necessary to exchange data (network variables and data points) between such modules. In the next stage of the development process, with the increase in the computing power and operating speed of microcontrollers (in the 2000s), universal programmable input–output modules appeared. Then, automation servers and other system modules have been introduced that support the processing of growing amounts of data at the object level [56–58]. As a result, especially in larger commercial and public buildings (e.g., hotels, shopping centers, offices, and university campuses), it became possible to build extensive automation and building management systems (BACS and BMS) with a fully distributed architecture. However, at the same time, the growing number of modules creating BACS and BMS forced the systematization of this architecture as well as the communication protocols. In [55,58,59], the authors describe and explain their most important elements, pointing to the progressive hierarchization of the BACS network architecture. According to the main assumptions, the overall architecture for a typical BACS can be organized into three layers/levels depending upon the functional hierarchy of the specific application:

- Field layer, the lowest one, where the interaction with field devices (sensors and actuators) happens, environmental data are collected, and parameters of the environment are physically controlled in response to commands from the system. Additional modules of sensors, stationary and mobile beacons with BLE, Z-Wave, and ZigBee wireless-communication technologies, are often used on this layer as well. They support mechanisms for the precise location of people and equipment in rooms and for monitoring environmental parameters;
- Automation layer, the middle layer, where data are processed, control loops are executed, and alarms are activated. It is also where processing entities also communicate values of more global interest to each other, and values for vertical access by the next management level are prepared (possibly aggregated);
- Management layer, the top layer, is where information from throughout the entire system is accessible, as well as where activities like system-data presentation, forwarding, trending, logging, and archiving take place. Moreover, vertical access to all BACS values is provided, including the modification of parameters such as schedules and long-term historical data storage. The possibility to generate reports and statistics is implemented as well.

With this concept, the progressive growth of data-processing tasks and services carried out at the highest Management Layer is clearly visible. However, the next stage of development of distributed BACS systems is not associated with progress in electronics, but with the rapid expansion of ICT networks, which over the last dozen years have been gradually reaching the management level and even lower levels in the architecture of BACS networks. Therefore, the key question is: how far this inclusion should go, whether TCP/IP protocols of ICT networks should dominate or perhaps completely take over communication and data handling in field-level networks? Are the protocols dedicated to field-level networks (ISO/OSI model), developed over many years and still strongly present in industrial and building automation and to be replaced by the expansion of TCP/IP, or should they exist together in a kind of symbiosis [20,60]?

In response, a broad, multiaspect analysis of the currently developed generic IoT concept is necessary, considering specific application requirements, security, privacy, and operational reliability of smart home and smart building systems.

2.2. IoT Structures and Technologies for Building Automation

The possibility of including TCP/IP communication channels in field-level networks has generated a multitude of application concepts at various levels of the existing architecture of BACS and BMS systems that address this topic by several engineering and scientific teams, along with additional marketing chaos. For example, the KNX Association and LonMark International, recognized organizations in the building automation industry, responsible for international open building automation standards, have launched information and advertising campaigns that the KNX [8] and LonWorks [9] standards are “IoT ready”. Similar information still appears in the materials of many manufacturers of modules for BACS, BMS, and smart-home systems [61–63]. Therefore, in the first years of this process, research, engineering, and methodological works were already carried out aimed at verifying the technical capabilities of TCP/IP transmission channels and the IoT paradigm based on them in the effective implementation and support of the efficiency of BACS, BMS, and smart-home systems.

Scientific studies from the first two decades of the 2000s indicated potential areas of IoT applications and attempted to define possible development concepts for distributed networks. Kortuem et al. [64] propose a concept of smart objects as independent nodes with awareness (ability to sense, interpret, and react to events occurring in the physical world) and interaction (ability to converse with devices, other nodes, and the user in terms of input, output, control, and feedback). They discuss a general approach to such a concept, without specification of application areas (e.g., smart home or building), analyzing the possibilities of building peer-to-peer (P2P) data-exchange networks based on such smart objects to implement more advanced control and monitoring functions as well as data acquisition from sensors, actuators, etc. It is very important to note the reaction of smart objects to events, which is a key element of smart home and building systems, defined as event-based systems. In turn, in [65,66], the authors already point to the potential possibilities of IoT integration in the structures of BACS and BMS systems. However, the proposed applications concern only the use of IoT gateway modules and integration servers to support the operation of distributed BACS network nodes (integrated within field-level networks) in the implementation of remote access, data acquisition, and visualization in external services and object-linking and embedding for process control (OPC) databases. Therefore, IoT technologies in this approach constitute an addition, without significant interference in the structures of existing and planned BACS and BMS field-level networks. For example, the IoT with a TCP/IP protocol is considered a crucial element of a standardization process of building automation protocols.

However, the second decade of the 2000s brings more and more analyses and technical developments of the BACS architecture concept using IoT technology in system integration and development trends for modern smart home and building systems. In conference proceedings [67], Jung et al. discuss the new version of the IPv6 protocol and its most important features, such as the larger address space, self configuration, quality of service mechanisms, and security, qualifying it for applications in BACS and BMS, and promising a better integration of building automation technology in the IoT. Moreover, they conclude that the transition towards IPv6 from IPv4 at the *Automation* and *Management Layers* opens new opportunities for several previously not realizable use case scenarios in BACS and BMS like (i) home and/or building infrastructure device maintenance, (ii) smart grids and energy efficiency with interconnected devices, renewable energy sources (RES) and dynamic load shifting, the energy pricing ready for transactive energy concept, and, finally, (iii) buildings integrated into business processes with advanced occupants monitoring, access control, and HAVC operation and lighting control. In this context, several technical aspects of IoT integration with different BACS standards (KNX, LonWorks, BACnet, and OPC) are shortly discussed with a use case study.

Going one step further, Lilis et al. [68] proposed a transitional design for BACS networks that integrate IoT technologies. Based on the BACS architecture with field-level modules with communication in open standards (BACnet, KNX, and LonWorks), the use of the Internet backbone, and the developments in the embedded electronics at a higher level of the network structure, the authors point out the possibility and necessity of successive implementation of the embedded web services, sometimes referred to as Web of Things (WoT). In this way, the control and monitoring functions of BACS systems become services implemented in the form of applications in IoT devices at the automation or management layer, with communication of signals from and to field-level modules. Moreover, the authors analyze the practical possibilities of implementing openBMS-class platforms by providing a palette of semantic web services with the wide adoption of IoT-based management systems. For this purpose, they propose the implementation of universal distributed embedded electronics modules at the automation layer. According to this concept, each of those modules is an always-listening participant of the sensor and actuator networks and provides gateway-like capabilities towards the computer network [69,70].

Bearing in mind all development aspects of the concept of integrating IoT technology in BACS and BMS networks, Figure 1 presents their most important elements and differences visible, especially in the middle layer—the automation layer.

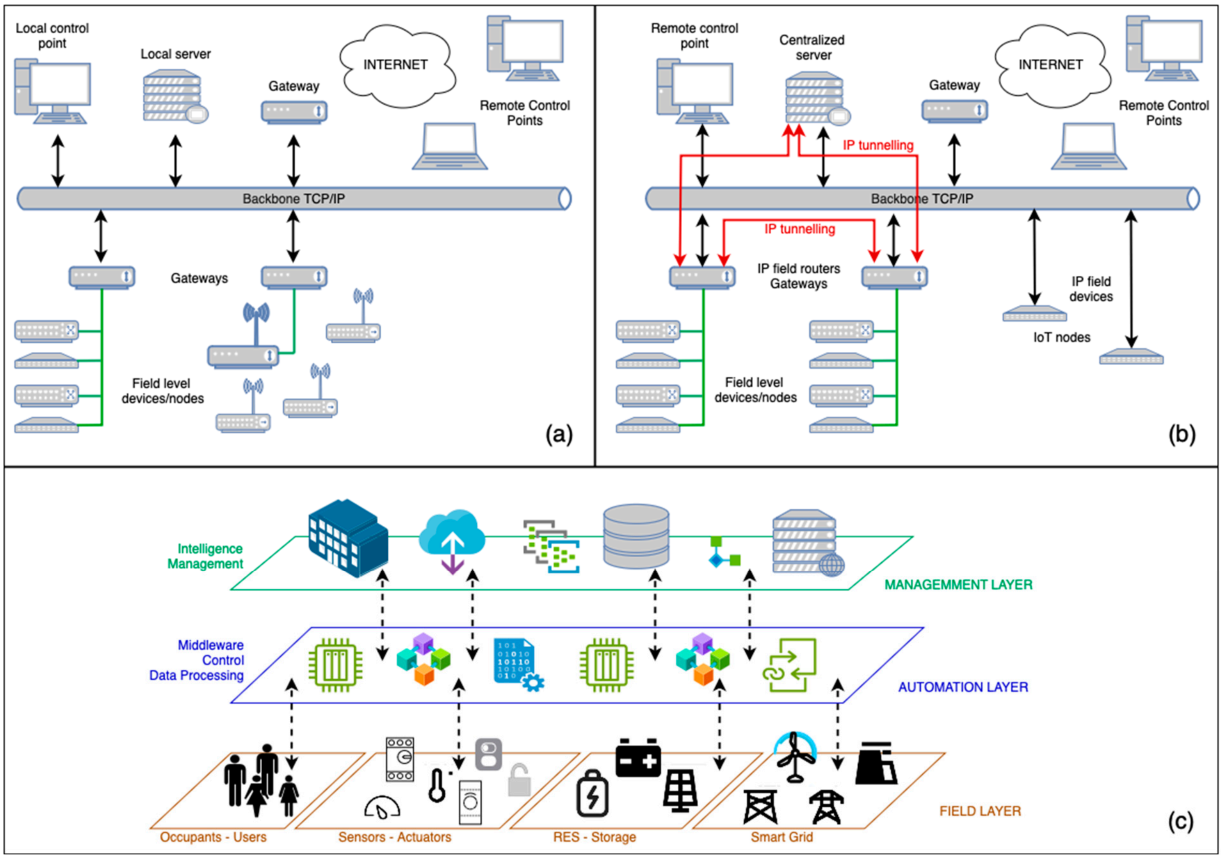

Figure 1. Schematic diagrams for two basic concepts of IoT development and application within the BACS and BMS architectures: (**a**) field-level devices connected by universal gateways to the higher network level using TCP/IP protocol and providing remote access [66]; (**b**) field-level devices connected by dedicated modules (automation servers, IP gateways) providing both remote access and data tunneling (IP channel integrated within the BACS and BMS architecture) [56,67]; and (**c**) additional distributed embedded electronics modules implemented at the automation level [68,69].

3. The IoT with Edge and Fog Computing in Buildings—Main Challenges

The turn of the second and third decades of the 2000s and until now is a period of rapid development of ICT network and cloud services. During this period, the widespread use of server resources (cloud) for storing and processing large amounts of data has been developing, basically, in all areas of industry, science, and social life. In the building automation industry, there are subsequent years of progressive integration of field-level networks with ICT networks and a trend toward implementing advanced control, monitoring, and management functions of an increasing number of elements of the building infrastructure. Moreover, the progressive implementation of energy-management algorithms, energy media, and the operation of local microgrids with RES and smart-grid services.

3.1. Service-Orientated IoT and Edge and Fog Computing in BACS and BMS

Such a significant development of functional concepts indicates new development trends in BACS systems in smart home and building applications. Simultaneously, the continuous development of IoT techniques and microcontrollers determines the need for organizational changes in BACS networks. In particular, this concerns the expansion of the ability to perform most of the analyzing and data-processing functions for monitoring and controlling the building infrastructure directly in the local network (within the building, campus of buildings, etc.). This is made possible by the computing power and memory resources of many modern distributed embedded electronics modules (automation servers, advanced routers, and gateways), integrated in the automation level of the

IoT network. These modules, usually located at the junction of the field and automation (middle) layers, create the so-called edge computing in the modern BACS with IoT-network nomenclature [46]. Edge computing can be defined as a computing approach that uses resources in the periphery of a network. In this way, it brings the computation closer to the nodes of the BACS at the network's edge to provide a minimal delay and lower latency period between the moments that the data are acquired by sensors and then sent as control signals for actuators within the BACS [40,71,72]. The ongoing development of this layer of the BACS network, in particular the exchange of data in the TCP/IP channels between distributed embedded electronics modules and their performance of local, advanced analytical and data-processing functions at the automation level, has led to the creation of a new paradigm and term, fog computing, in the modern BACS with IoT networks. Fog computing is a distributed network resource that performs functions using local network resources but is also open to external services outside the local network—in the cloud [45,46]. Fog computing, therefore, operates at the automation and management levels, which are still supported by the local network and external resources. Hence, the fog element in the name indicates a kind of blurring of the integrated network layers [48,49,51,71]. The technical and organizational aspects of IoT networks presented in this subsection have significantly influenced the architecture of modern BACS and BMS systems in applications for smart homes and buildings. The general structure of such a network, highlighting the most important elements and levels, is shown in Figure 2.

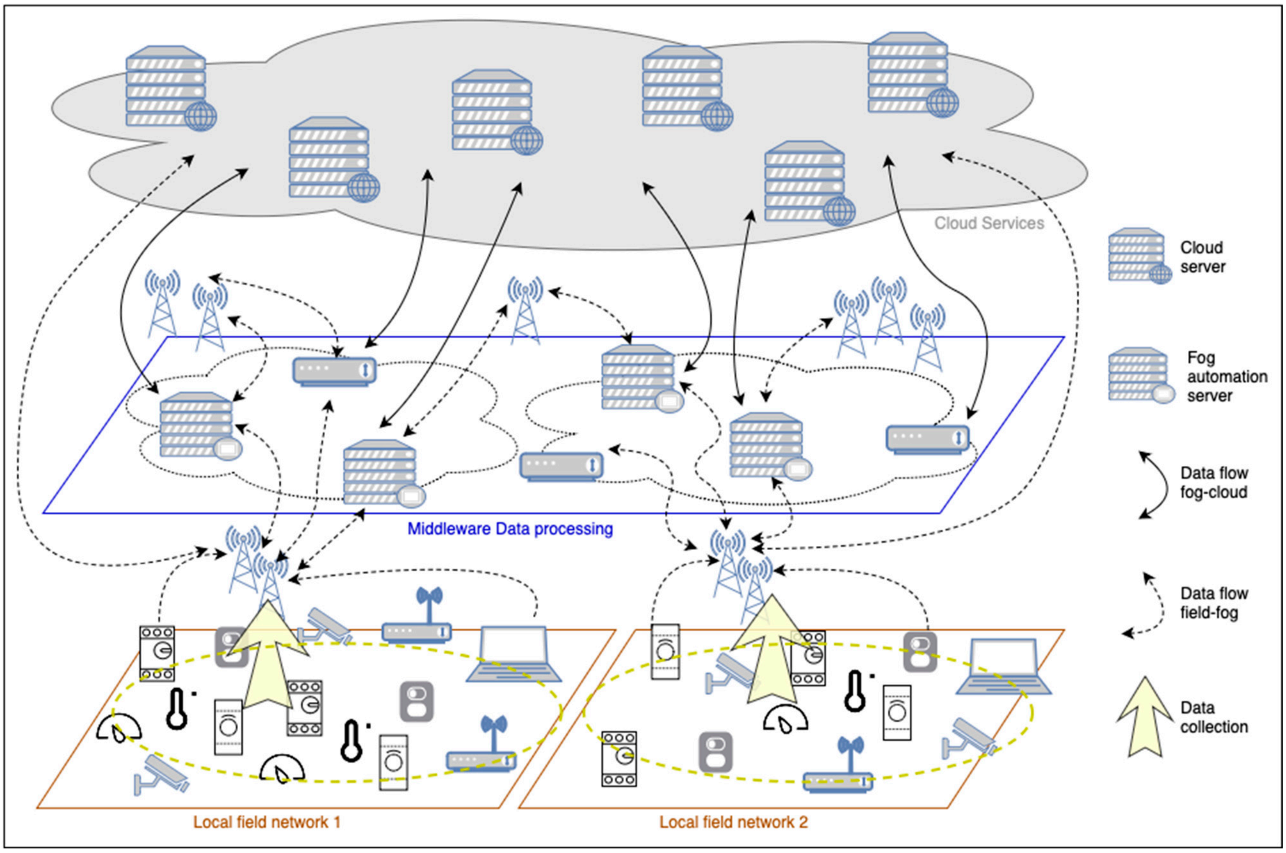

Figure 2. Structure and data flow in the network with field-level local networks, fog level, and cloud level [51].

In addition, BACS and BMS networks with such a structure, using distributed modules with TCP/IP communication in the edge and fog computing structure, create an environment for a service-oriented IoT [47] and a new Building as a Service (BaaS) [73] strategy. The first one is more general in nature; in the literature, it is referred also as Fog of Everything (FoE) and Internet of Everything (IoE) and focuses on the ability to use IoT technology in the implementation of services for four main areas: processes, data, people, and things. Formally, this approach refers to an ecosystem of edge modules that autonomously share and self-manage their limited resources in order to achieve the system goal (e.g., implementation of dynamic control, monitoring, management functions, etc.) [74].

The second one is more detailed and refers directly to the development concepts of BACS and BMS systems, in particular in smart-building applications. According to [75,76], buildings, in particular nonresidential ones equipped with BACS and IoT distributed networks integrated with fog and cloud computing, can be perceived in the BaaS convention, defined as the demand-oriented deployment of resources and assets, respectively. With this approach, buildings become platforms of information for providers and consumers. The focus moves from functions and services available in a building with BACS and BMS to view the building as a service-dominant logic-based asset. In this way, facility management (FM) is, in practice, a process of dynamic data management and data mining in order to adjust the operating conditions of building infrastructure devices to the current needs of users and changing environmental parameters (e.g., temperature, daylight level, energy tariffs, etc.). Moreover, it opens the way to building a framework of open data-processing platforms to provide specific services to users and infrastructure elements based on measurement data and device operating parameters.

Wildenauer et al. [75] also point to the inclusion of the BaaS and IoE approaches for enabling a digital twin (DT) tool based on building information modeling (BIM), which is becoming mandatory in several European states. In this context, it should be emphasized that the latest Energy Performance of Buildings Directive (EPBD 2018) [77] and the related technical report [78] define the smart readiness indicator (SRI) along with guidelines for verifying this readiness based on the services offered and possible to implement in the building. The first verification analyses of the usability of this indicator and related services in buildings are carried out as part of research and engineering works in order to develop mechanisms for applying the indicator's guidelines in real applications of buildings as well as energy microgrids with RES and energy storages [44,79–81].

3.2. Big-Data Processing and Cloud Computing

An aforementioned approach to BACS with IoT as a framework of an open data-processing platform requires the integration of numerous sensor and actuator modules as well as automation servers at the field and automation layers. Moreover, it is necessary to organize network connections of edge modules and computing infrastructure with external resources in the cloud. This entails the need to ensure efficient transmission and processing of large data resources while maintaining the time regime (real time) so that the implementation of BACS and BMS functions and services takes place essentially unnoticed by the building users. At the same time, in recent years, there has been a rapid increase in the popularity of data collection and processing services in the cloud—external servers usually operated by external entities or at the disposal of suppliers of smart home and smart building systems. This situation also affects designers and integrators of BACS systems with IoT, who often decide to implement cloud-centric systems, where there are basically only two levels of network structure, field and management (cloud) layers, and all more advanced functions and services in system are implemented in external cloud resources [82,83]. At the same time, they rely largely on data processing and protection tools offered by external administrators of such cloud services. However, this is not always beneficial, especially considering that many advanced services can be provided by modern BACS and IoT modules directly at the automation layer, close to the field layer modules. This solution naturally increases data security and reduces the load on network-communication channels. Therefore, in concept research and application case studies of modern BACS and BMS with IoT, solutions based on more advanced multilevel structures of system networks are considered and developed. The key element of these analyses is the development of guidelines regarding the areas of implementation of BACS and BMS functions and services in the network structure (what levels, between levels) and the methodology for the effective organization of network variables and data objects binding (interoperability, integration) to provide control and monitoring services. Considering the possibility of moving away from a cloud-centric organizational strategy, Chen et al. [84] propose an original cloud–fog computing architecture for information-centric IoT applications providing a classification of IoT applications and scheduling computing resources. Moreover, a developed scheduling mechanism optimizes the dispatch of cloud and fog resources regarding minimum cost in a cloud–fog computing environment. In turn, Sahil and Sood [85] discuss cloud–fog architecture implemented in a specific application, the panic-oriented disaster evacuation system in smart cities, with a particular analysis of the effectiveness of the proposed system-data-processing algorithms for various functional priorities (e.g., accuracy and sensitivity) in a very demanding time regime.

Research and development work is also carried out from a second perspective focused on the lowest levels of the network structure. In paper [4], the authors proposed a model and algorithms for handling modules with video cameras distributed at the field layer, with identification and classification services of recognized objects implemented at the automation layer in edge modules and a local workstation with the Microsoft Azure IoT Platform. Research focused on the functional capabilities of this solution and measurements of the system's effectiveness were carried out with the results discussion. In other studies, Huang et al. [47] propose an edge intelligence framework to build smart IoT applications. The project they developed is based on an extensive automation layer, with many edge modules cooperating to support local groups of field devices. A characteristic element of the concept is virtualized IoT services, which enable hardware-independent application design and simplify IoT services composition using different field-layer (physical) devices without redefining applications. This is an element of the ongoing strategy of organizing fog computing at the automation layer, within the local system network. Further development of the concept is proposed by Nasir et al. [39] by employing edge devices as a computational platform in terms of reducing energy costs and providing security, as well as remote control of all field devices and appliances behind a secure gateway. Moreover, in the automation layer, in addition to edge modules (nodes), they define fog nodes based on the powerful Jetson Nano device [86]. The platform is open for integration with external cloud services but is considered only as an additional tool to perform the most advanced processing, data analysis, and machine-learning services.

In turn, in paper [40], Lacatusu et al. analyze several design variants of the monitoring and control system for the infrastructure of a smart-buildings complex, based on edge computing and containers with additional cloud-computing services. Importantly, the authors conducted a comprehensive performance evaluation of design concepts using testing environments with two architectural options, (i) centralized (a cluster hosted in a public cloud) and (ii) decentralized (a similar cluster deployed in a local datacenter). They executed tests considering different numbers of edge nodes, corresponding to real application cases, namely a small apartment, a house, a small residential building, an office building, and a complex of smart buildings.

Finally, the research and engineering work of the last few years has focused on the development of various comprehensive concepts for the organization of smart home and building systems with the IoT–edge–fog–cloud architecture. For instance, in [3,51,87], the authors propose similar structures and frameworks for BACS and BMS networks with IoT, using in particular the new capabilities of edge and fog computing modules. In all cases, regardless of the application area, the structures of the automation layer are expanded, where operations are carried out by providing services such as data aggregation and analytics, security, access control, self healing, and self managing. The general diagram of such a network layer structure is shown in Figure 3.

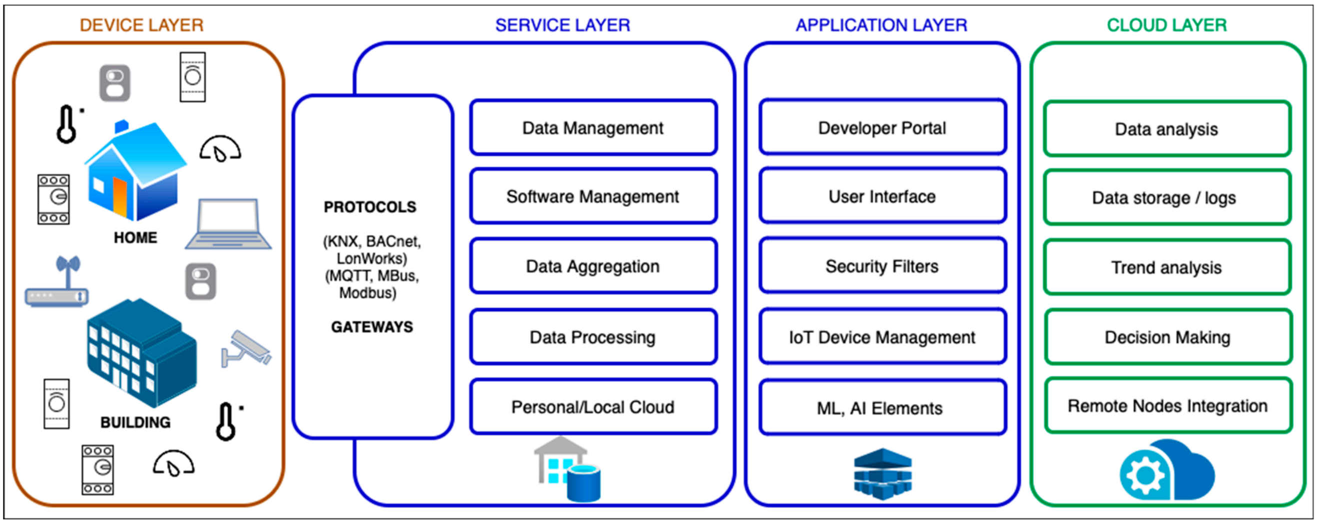

Figure 3. Advanced layer structure of BACS, BMS with IoT network, including big-data processing and cloud services [3,51,87].

For these solutions, the use of various communication technologies and the possibility of building network nodes based on universal modules with microcontrollers (e.g., Arduino and ESP) or a class of microcomputers (e.g., Raspberry Pi and Beagle Bone) are analyzed. Using the results of these analyses, engineering teams carry out tests aimed primarily at improving efficiency and reliability while rationalizing costs and resources used.

With this approach and the clear development trends of edge and fog computing in BACS and BMS systems, the issues of selecting communication protocol techniques and implementing data-security mechanisms, certainty, and unambiguity of communication become very important. In the context of the variety of available communication protocols, both wired and wireless, a comprehensive analysis of their usefulness and application potential was carried out in [71]. Furthermore, a broader analysis of security issues and data-transmission reliability was carried out in BACS and IoT edge computing networks in smart-city applications in [7].

3.3. Cybersecurity, Privacy, and Blockchain Solutions for Distributed IoT in Buildings

It should be noted that the aforementioned developments of new structural concepts of BACS and BMS networks in smart home and building applications, in particular the progressive distribution of IoT nodes and edge modules at the automation layer cooperating with external cloud services, resulted in a greater "openness" of the BACS network structure for new threats related to their inclusion and progressive integration into commonly used TCP/IP networks. Moreover, new structures of communication and access to data in the fog computing networks have been created, generating completely new categories of threats. According to [88], traditional conventional security mechanisms will not be designed or developed to secure technology such as the IoT. Therefore, it is necessary to develop and introduce innovative solutions in the field of data security and reliable trusted communication in the organized structures of a smart home and building network. These issues are the subjects of numerous research and technical analyses.

One of the most generalized analyses is presented in [38], where the authors indicate the most important issues related to the security and privacy of IoT networks. They discuss (i) confidentiality (data secrecy which guarantees the reliable transfer of data); (ii) data integrity (prevents corruption or alteration of data during transmission); (iii) availability/disposeability (ability to provide sufficient network and data processing resources when necessary), and (iv) authenticity (unique identification of users and resources authorized to operate on a given network). Moreover, they indicate significant challenges resulting from the development of IoT networks affecting security and safety issues. According to the authors, there are five main ones [38].

- Heterogeneity of devices and communication, resulting from the coexistence of various modules/nodes in one network structure (from small sensors and relays to large modules of automation servers and data servers), and the fact that they are produced by various manufacturers, often with different hardware architectures, supporting various types of software tools;
- Integration of physical devices; the result of the aforementioned 'openness' is that an attacker is potentially able to communicate with more devices than before. If he breaks the home/building/local network protection, he is able to manipulate the lighting system, lock doors, control HVAC, etc.;
- Constrained devices, the feature of many IoT devices resulting from a tendency to reduce the cost of their production. As a consequence, IoT devices have limited resources, memory space, low bandwidth, etc., and these considerably reduce the possibility to implement conventional security techniques;
- Large scale, since, currently, there are more computers and other IoT devices connected to the Internet than the number of humans on the globe, and the management of so large number of smart devices is a very demanding task and inevitably raises security risks;
- Privacy, IoT devices by their nature operate in a distributed structure, allowing communication for various wired and wireless technologies. This approach allows for interaction everywhere and data communication with many other BACS network nodes and edge modules in order to provide various services with different scopes and resource uses. The openness and flexibility of this structure generate additional privacy risks.

This is, of course, a very general summary. More threads emerge in detailed analyses. Particularly noteworthy is paper [89], where Parikh et al. consider security and privacy risks for all three of the most important levels of IoT networks, namely cloud computing, fog computing, and edge computing. The result of the analyses is a classification of the complexity of problems and preliminary proposals for solutions but without any technical or technological indications. In turn, paper [45] contains an overview of proposed solutions that increase the level of security and privacy in edge and fog computing structures. Laroui et al. provide a synthetic summary of the literature devoted to efforts to improve security and privacy in IoT networks, along with a brief discussion of the proposed models, mechanisms, and tools. Moreover, they discuss future research directions in this area considering the balance between openness and ease of use of the IoT networks and the need for a high level of their security and reliability.

From the point of view of BACS and BMS systems with the IoT, the most important are countermeasures dedicated to fog and edge computing integrated at the automation layer, usually within a local subnet. Such countermeasures are described by a detailed literature review by Alwakeel A. in [90]; in particular:

- For fog computing
    a. Encryption techniques;
    b. Decoy technique for authentication of data;
    c. Intrusion detection system for denial-of-service attack (DoS attack) [91] as well as port scanning attacks;
    d. Authentication schemes, where the fog computing network enables users to access the fog services from the fog infrastructure if they are well authenticated from the system;
    e. Blockchain strategy, it can prevent various malicious attacks in the fog network, including man-in-the-middle attack, DoS attack, and data tampering.
- For edge computing

a. Edge node security;
b. Full-time monitoring of edge nodes;
c. Encryption with secret keys and attribute based [92];
d. Intrusion detection system;
e. User behavior profiling;
f. Cryptographic techniques with smart secret keys;
g. Data Confidentiality, for example with a privacy-preserving QueryGuard mechanism [93].

One of the most frequently discussed and analyzed solutions that is intended to support the implementation of the most advanced security and privacy elements is blockchain ledger technology [45,90]. In relation to the IoT paradigm, it is explained in [94] that blockchains, by definition, rely on a public directory acting as a common transaction information database for devices (nodes), edge modules, and automation servers. Furthermore, in [95], Moniruzzaman et al. discuss the blockchain-based smart-home ecosystem, with the framework presented in Figure 4. According to them, it is a four-layer conceptual framework consisting of four layers, namely the (i) IoT data sources layer, (ii) blockchain network layer, (iii) smart-home applications layer, and (iv) clients layer.

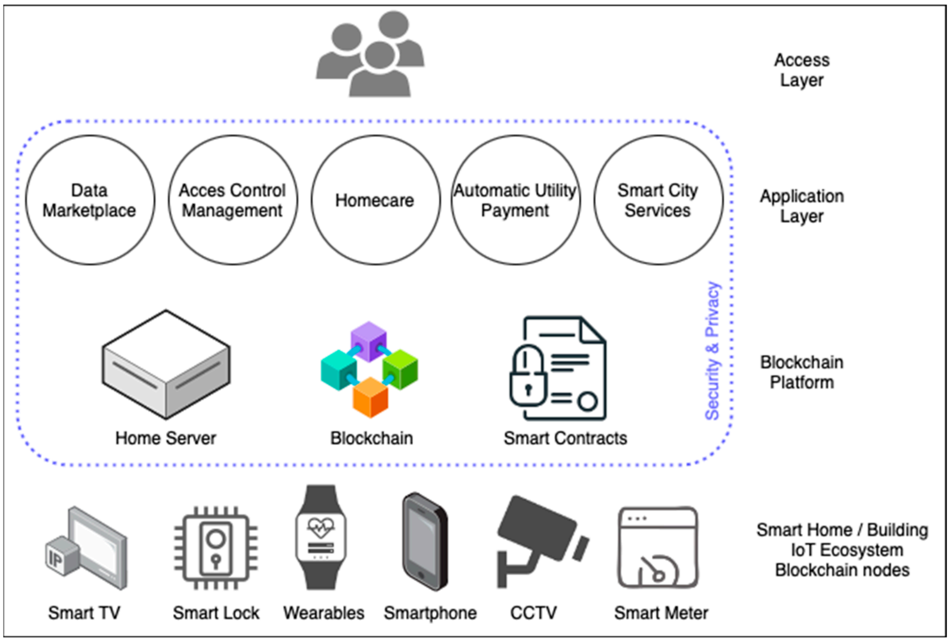

Figure 4. A four-layer application framework of a blockchain-based smart-home ecosystem proposed and discussed in [96].

Sensors and actuators located in the first one generate and/or use data consolidated and stored in edge modules (servers) or a decentralized platform such as the second one—a blockchain. All of the events and acts of the sensors and actuators became smart transactions used to realize services. What is characteristic is that time is an indestructible database that is placed in a new transaction and divided into a block hash chain. In this way, many copies of blocks are made and saved in the extracted node protocol. Moreover, hash values cryptographically connect blocks, and edge modules (servers) may be considered miners, which are responsible for verifying and adding new transactions to new blocks while smart contracts follow predefined rules and facilitate the decentralized transactions [94,95]. This organization of data processing as a transaction with a trace in the block structure fits naturally into the framework of distributed BACS and BMS with IoT networks [96]. Additionally, it opens the way to easier and more reliable integration with external services, for instance in the community microgrid frameworks suggested in [97].

Importantly, the more distributed the network nodes in such a structure, the higher the security level due to blocking verification procedures in the nodes. Therefore, the distribution factor, previously identified as reducing data security, becomes an advantage with this approach. The pros and cons related to the implementation of blockchain technology in IoT networks in various application areas, including smart homes and buildings, are discussed in [98,99], considering security and privacy aspects as well, and indicating the added value of such an approach. A detailed analysis of the transaction workflow along with the accompanying tools and methods of data protection in the fog and edge computing network structure, is presented in [100]. In the conclusion section, the authors also provide a comprehensive review of research work focused on the possibility of increasing the level of security and privacy in IoT networks, along with an indication of various limitations. Some of the latest research suggests innovations in the integration of blockchain technology in IoT networks, allowing for overcoming the limitations of the classic approach, such as scalability, storage and bandwidth, transaction charges (checking by miners), data privacy (sharing every node), and network size (all nodes within the network). In [88], Alshaikhli et al. introduce an IoT application (IOTA) distributed ledger technology that can provide unlimited scalability specifically suitable for the IoT with fog and edge computing. In particular, this technology provides fully distributed data transactions without a central authority unit, microtransactions in real time with zero fees, a new scalable distributed ledger mechanism, and masked authentication messaging with advanced encryption of data.

4. New Ideas, Concepts and Trends

The generic IoT concept for smart buildings and field-level automation should be considered first of all in the context of needs and facilitations in organizing and integrating increasingly distributed network nodes as well as new ideas and development trends of smart building systems with IoT. Since IoT technologies and application areas are still undergoing rapid development in many areas, this study selects several of the most important aspects that seem to be important in relation to smart home and building systems.

4.1. Machine Learning and Artificial Intelligence

The development of modern techniques for collecting and processing big data has allowed for the effective implementation and use of ML and AI mechanisms, in particular supporting the organization and functioning operation of automation systems. According to Djenouri et al. [101], in the context of BACS and BMS, ML techniques could be used to solve fundamental problems, such as predicting occupant behavior and preferences and forecasting energy demand and peak periods, which are difficult to solve with traditional programming, but potential solutions can be achieved from advanced and fast data analyses. They reviewed several research and studies and discussed potential areas for ML applications in two aforementioned categories:

- Occupant-centric solutions
    a. Occupancy detection, prediction, and estimation providing essential information for advanced control of several subsystems like HVAC;
    b. Activity recognition to provide better control scenarios, tailored to increased or limited user activity, e.g., in different zones of the building;
    c. User preferences and behavior to provide well-tailored thermal and lighting comfort, considering individual or group user preferences, as well as operating scenarios for home devices and building infrastructure tailored to the most common recurring user behaviors;
    d. Authentication schemes, where a fog computing network enables users to access the fog services from the fog infrastructure if they are well authenticated in the system;

    e. Blockchain strategy, it can prevent various malicious attacks in a fog network, including man-in-the-middle attack, DoS attack, and data tampering.
- Energy/device-centric solutions
    a. Energy profiling and demand estimation in the context of using BACS and BMS monitoring and control functions to improve the energy efficiency of buildings, in particular, those incorporated into the structures of local energy microgrids and prosumer installations [12,102];
    b. Appliance profiling and fault detection to track and identify different buildings' appliances, as well as detect anomalies/failures in the different components of the energy management system. Moreover, this approach allows support of the DSM and DSR mechanisms of transactive energy [103,104].

These two categories are mostly discussed in the context of ML applications within smart homes and buildings. In [105], the authors analyze in detail various technical and functional aspects of human activity recognition in smart homes using algorithms for IoT sensor networks, considering the pros and cons of different ML methods and tools dedicated for various smart home and building applications. However, in [106], Suman et al. point out that, in turn, advanced IoT and BACS devices may impact the behaviors of people in buildings. Based on human and various thermal and environmental models, the authors analyze their possible mutual impact, in particular, changes in human behavior depending on changes in building infrastructure control scenarios and comfort parameters.

In turn, in [107] Machorro-Cano et al. present a HEMS-IoT, a big data and machine learning-based smart-home energy-management system to provide home comfort, safety, and energy savings. ML techniques and big-data processing technologies are important in this solution since they help to analyze and classify energy consumption efficiency, identify user behavior patterns, and offer increased comfort at home with rational energy usage. Additionally, in [108], the authors identify the most essential BACS with IoT-enabled factors that sanction a need for ML, as well as AI integration with smart homes and buildings to provide energy-efficiency improvements and facilitate energy management. Research, analyses, and case studies are carried out in this area using advanced functionalities and communication techniques [41,80,109–111].

Another issue is the possibility of using ML mechanisms with AI elements to recognize, classify, and service BACS and IoT modules and network nodes. Cvitic et al. [112] propose an original approach and an ML-based IoT device classification model considering various sets of data and different data traffic models. Furthermore, considering the growing use of BACS with IoT solutions, especially with edge and fog computing, Huang et al. [47] note that real-time detection of unexpected, emerging, or spontaneous situations is important for increasing the reliability of the network and improving its maintenance. This approach makes recent data more valuable than historical data for the learning models, which also determines the need to develop ML mechanisms with a shorter time window for analyzing data sets. All these issues indicate the growing importance and even indispensability of ML technologies and methods in BACS, BMS, and IoT systems in the coming years. Moreover, research is already being conducted to develop new trends in ML development. Due to the increasing computing power of edge and fog-level network nodes, a federated learning (FL) approach is proposed [50,113,114]. In this concept, the nodes within the IoT network get involved in the training and inferring process, keeping the raw data within themselves and sending only the results of local training processes performed on these network nodes, to maintain privacy and reduce communication overhead. Importantly, FL mechanisms based on the dispersion of network nodes and their computing power are indicated as important elements of the development of blockchain technology in the field of more advanced data security and privacy mechanisms in BACS networks with IoT [115–117].

However, the AI functions and solutions are particularly considered in the context of support in the integration processes of extensive BACS system networks with IoT, supporting very diverse functional and infrastructure subsystems of buildings and homes. First of all, AI integration is important since, in classic BACS and IoT networks, the design and architecture development of each control function, and the rule only works in one subsystem (e.g., HVAC, lighting, security, etc.); there is no interoperability between these subsystems (or it is very limited). Furthermore, as previously stated in Sections 1.1 and 1.2, the monitoring and control functions of these systems are often aided by other modules such as sensors and beacons with wireless-communication interfaces that do not support the TCP/IP protocol directly. This requires the use of additional gateways or data concentrators.

Considering this, the model proposed in [3] facilitates and allows the integration of new digital services based on BACS and IoT nodes, providing deeper interoperability of the different subsystems and introducing new services based on ML and AI techniques to homes and buildings. The authors have implemented the model and verified it in tests. Moreover, in [118], Panchalingam et al. describe several smart-building domains that should be considered for integration with AI techniques in relation to those techniques. They suggest and discuss what research on AI techniques should be conducted to improve safety, BACS and IoT systems design, control logic, and energy efficiency in buildings as well. The similar aspects are analyzed in [119,120], considering not only functional and organizational aspects, but technical and architectural as well.

The synthetic summary in graphical form in Figure 5 indicates the areas in which the use of ML, FL, and AI techniques is observed and suggested.

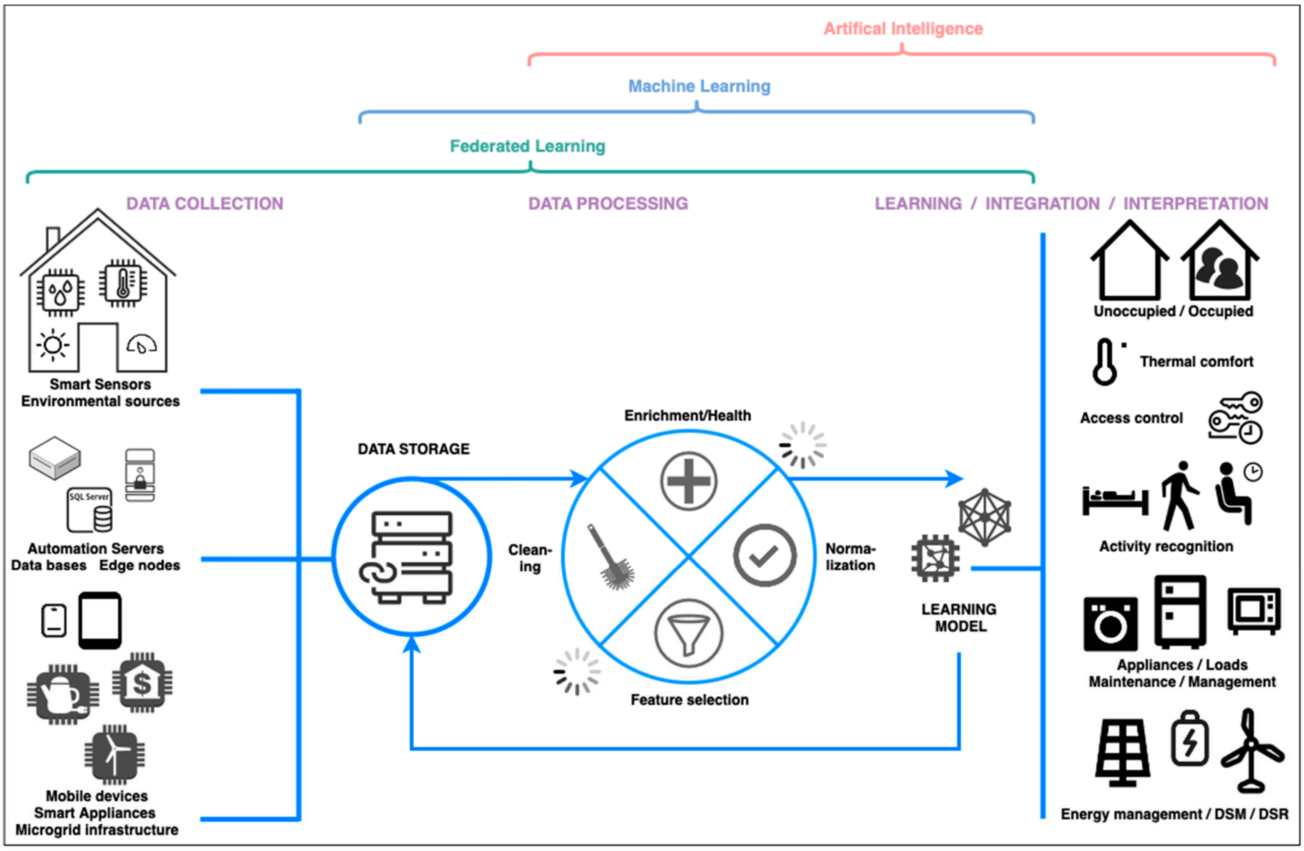

Figure 5. The BACS with IoT systems areas for implementation of ML, FL, and AI techniques, methods, and tools (based on [101]).

4.2. Tactile Internet and Digital Twins with Distributed Automation Networks

All these methods and technologies, namely ML, FL, and AI, become the basis for the implementation of new functional possibilities and the development of emerging trends of BACS and BMS systems with IoT. The author has selected two, namely Tactile Internet and Digital Twins, which are, in his opinion, currently the most important trends that are both part of the development of a new philosophy of using smart home and building systems and as operational maintenance support techniques, especially for large BMS with IoT systems in smart buildings. The importance of the emergence of these development trends is indicated by the increase in the number of scientific publications observed since the mid-second decade of the 2000s, in particular those resulting from research and development projects. In the publication databases of ScienceDirect (Elsevier), Springer, and IEEE Xplore, 80% of publications on the topic of "tactile internet in smart applications" are in the years 2017–2023. Of which, the years 2020–2023 amount to almost 300 publications per year. A similar proportion applies to the recognized bibliometric services Web of Science and Scopus. In turn, in relation to the second emerging trend, Digital Twins in smart buildings, the analysis of the number of scientific publications in the ScienceDirect, Springer, and IEEE Xplore databases indicates an even narrower time spectrum, 2019–2023, with a rapidly growing number of publications (for example in ScienceDirect in 2020: 462, in 2021: 714, but in 2022: 1094, in 2023: 1463). In the Web of Science and Scopus bibliometric services, the first single publications on this topic were recorded in 2017–2018, and in 2020–2023 there are already almost 200 publications per year.

The first of the discussed emerging trends is the Tactile Internet or Tactile Internet of Things (TIoT), considered the second generation of the IoT to support the transfer of haptic data (what is sensed by the skin) and kinesthetic data (muscle movement), in addition to audio, video, and images as tools for the human–smart home system interface [50,121]. In its most basic approach, TIoT involves wireless communication (5G and Wi-Fi) and classic wired channels to control real and virtual objects (actuators) by humans in real time. By enabling the control of the IoT nodes in real time, it also provides haptic sensations to create a new extent for human–machine interaction in homes, buildings, and industry [122,123]. The assumptions of the technical organization and architecture of TIoT systems are currently the subject of research and development work, but, as Fanibhare et al. [122] point out, crucial design goals can be achieved by placing TIoT nodes close to each other, which is possible with a distributed and decentralized architecture dependent on recent technological advancements, such as edge and fog computing. Therefore, modern, fully distributed, BACS and BMS installations with elements of fog and cloud computing services are becoming a natural implementation environment for TIoT. In particular, the development of user interfaces based on virtual reality (VR) and advanced applications for monitoring the activity, behavior, and health parameters of occupants is expected [122,124]. However, the implementation of user interfaces and functions in the haptic and immersive real-time interaction regime introduces new requirements for the data communication network, both in terms of its speed and throughput. In TIoT applications, a response time to events of 1 ms is required, much shorter than in the case of audio (100 ms) or video (10 ms) interfaces. That is why fog computing and FL technologies are becoming so important for the effective implementation of the TIoT concept, supporting mechanisms of local processing of larger data volumes and transmission of the results of analytical tools [50,121–123].

The second selected emerging trend is the Digital Twin (DT) environment, the concept of which is being developed for many industries and the building industry. It is usually discussed in relation to BIM techniques, which are based on technical data and operational parameters of the building for the purpose of modeling its architectural, installation, and utility structure. According to [125,126], BIM is used in architecture, construction, engineering, and facility management to facilitate the planning and analysis of various scenarios and building organization concepts as well as clash detection, lean construction, cost, and time estimation. However, the BIM concept does not include the element of data dynamics and the related predictive capabilities. In [125] the authors point out the two most important differences between DT and BIM, namely (i) the BIM was designed to improve the efficiency of design and construction, and still is used in these processes, but the DT is designed to monitor physical assets and improve their operational efficiency and provide predictive maintenance and (ii) the BIM was not designed to work with real-time data; therefore, it is used for design and construction facility management, whereas the DT is a dynamic environment, with support for real-time data and ML and AI. Moreover, in [127], Hadjidemetriou et al. describe building DT architecture separating four phases:

1. Collection of data and information regarding the geometry, materials, and equipment characteristics of the specific building of interest. This information is necessary for modeling the building;
2. Collection of live measurements from sensors and electrical meters installed in the building to monitor its real-time operating conditions. In this context, modules with wireless-communication protocols, such as BLE, Z-Wave, and ZigBee, can be used at the field level, along with the required infrastructure for integration into the IoT TCP/IP network [128–131]. Additionally, live weather data could also be collected. These live data are directly incorporated as inputs into simulation tools to replicate the building's operating conditions in real time;
3. Simulation tools with model-based modeling are incorporated to simulate building control and monitoring systems. Intelligent algorithms can also be used to calibrate the building parameters in order to achieve better comfort and/or improve energy efficiency;
4. Development of a software platform to integrate the three previous phases. That platform is responsible for the proper data exchange and the successful real-time execution of the simulation tools as well as for integrating monitoring and control applications and investigating different what-if scenarios.

This architecture is presented in the graphical form in Figure 6, published and described in detail in paper [132]. Moreover, the dependencies between the BIM and DT techniques, in terms of their use in distributed systems with IoT, are analyzed in paper [133].

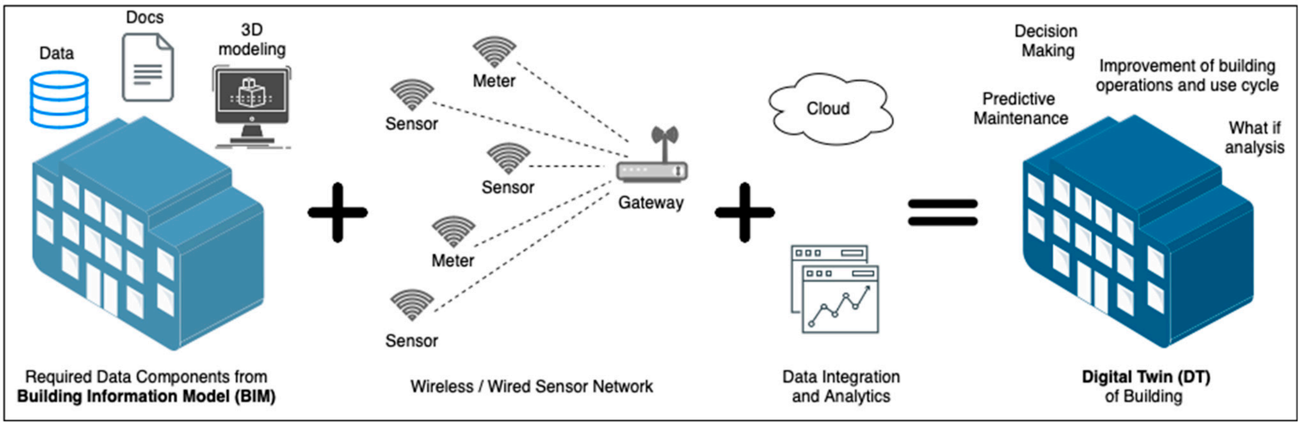

Figure 6. Essential components of building DT architecture [133].

From the analysis of the DT concept for buildings, it can be clearly stated that this is an environment requiring the involvement of all existing technologies and development tools of distributed BACS and BMS networks with edge, fog, and cloud computing elements. Thanks to them, it is possible to collect information about the operating status of the building's infrastructure, users' behavior and activity, and conduct active energy-management mechanisms, demand and load prediction, and provide control and monitoring functions [125,126].

4.3. IoT Technology and Maturity Assessment

The multitude of technical solutions and potential frameworks of modern network-automation systems with IoT technologies add complexity and raise questions concerning facility management strategies, organizational structures, and technological capabilities in the implementation of basic or advanced functions of monitoring, control, management of buildings, home infrastructure, etc. Additionally, many existing and operated buildings are equipped with very diverse IT systems, field-level networks, proprietary control systems, and other platforms supporting building management and BMS tools. In such a situation, the transition to modern IoT technologies and practices in order to streamline and improve the capabilities of effective building management is difficult and, above all, requires preliminary sorting and assessment of BACS, BMS, IoT technologies, and tools available to the user or building manager.

Therefore, in recent years, efforts have been made to develop IoT readiness assessment methods and tools. They focus, in particular, on the evaluation of two areas, namely the technical and organizational conditions of network systems in buildings, in terms of the possibility of their use in the development of infrastructure for comprehensive smart home and building systems with IoT. In [134], Arsenijevic et al. describe four possible methods for assessing the technological maturity of the IoT with varying levels of detail. The most important verification factors were analyzed, in particular, those related to the network structure (centralized or distributed), available computing power and data analytics tools, diversity of standards, and data-transmission protocols in the system, and also the readiness of the IT team to support new networks with edge and fog elements and cloud computing. In turn, in paper [135], Metwally et al. analyze these methods in detail, along with additional technical and organizational aspects relating directly to IoT applications in BACS and BMS. As a result, they proposed their own scale and indicator for assessing IoT readiness, with five levels of advancement:

1. Low IoT level, larger manual, low automatic control at the building level (local automation);
2. Mid-IoT level, automatic control at the building level (centralized automation), firstly emerging of DALI controls for lighting as well as field-level sensors for some control functions;
3. High IoT Level, automatic control at the building level (distributed automation), with networked sensors and modules and nodes to control most systems' functions with the performance analysis;
4. Fully IoT level, automatic control across all buildings/site levels (distributed networked automation) with networked sensors, all modules and nodes to control most systems' functions with the performance analysis also perform a predictive decision making.

The authors of paper [1] where, after a comprehensive analysis of existing methods to verify technological maturity and readiness for IoT solutions, proposed a four-level IoT assessment model, but with an additional level of zero. This model, however, relates mainly to organizational issues of preparation of staff and teams operating the network infrastructure and their awareness of system transformation, and to a lesser extent to technical and technological issues; although, of course, it does not ignore them.

In the context of the development of BACS and BMS platforms with IoT, it should be emphasized that the mentioned models and indicators complement the standards and studies regarding the selection of basic and advanced functions of home and building automation—standards EN 15232 and ISO EN 52120 [136,137]—and the assessment of the readiness of buildings for intelligent solutions and smart grid networks with the Smart Readiness Indicator (SRI)—EPBD directive [77]—and technical report [78].

5. Generic IoT Framework—Concept, Development, and Discussion

Bearing in mind all the technical and organizational aspects analyzed in Sections 2–4 of this review, the author proposes systematizing the most important elements relating to the technical, organizational, and conceptual issues, from the perspective of developing the concept and implementing the so-called generic IoT [138–140]. Wang W. et al. in [138,139] discuss for the first time the general concept of generic IoT, focusing on optimization issues and essentially reducing the size of data necessary for transmission between IoT network nodes. The approach they have developed and tested allows for more effective data handling by devices with limited resources and computing power. Moreover, they indicate that achieving integration both on a device and semantic (data) level for physical objects and services is possible thanks to the virtualization of middleware environment objects (edge and fog computing). With this approach, the handled data objects and integrated network nodes become universal, increasing the freedom of their connection and processing. A similar strategy for developing generic IoT is undertaken by Ali Z. et al. [140] who developed the thread of implementation of a number of data-processing services and information about network modules in the middleware environment (data acquisition, device heterogeneity, service management, security and privacy, interoperability, scalability, flexibility, data processing, and visualization). Considering the rapid technological progress and the increase in the possibilities of local data processing of edge and fog network nodes, they discuss for the first time the possibilities of implementing advanced data-processing mechanisms, including AI functions, in the middleware environment. They verify their proposals by analyzing the results of implementing the proposed mechanism in a smart-city application. However, all the publications discussed above indicate the dependence of the concept of generic IoT on many different factors, including policy, standardization, and development of innovative technologies (research and development), conditions, and requirements of specific applications, as well as the technological possibilities of supporting increasingly advanced mechanisms and algorithms for data handling at the middleware and object level.

Therefore, since designing an advanced framework for generic IoT systems in the context of building automation and smart-home systems involves careful consideration of various elements to ensure seamless integration and optimal functionality, the author of this paper decided to review and consider them, proposing holistic generic IoT framework dedicated for this type of applications. In the next subsections, there is a structured framework proposed, outlining both the mandatory and optional elements, as well as considering specific requirements for smart home and building applications, including edge, fog, and cloud computing. Moreover, the main fields of potential research and development work are suggested as well.

5.1. Mandatory Elements of the Framework

The elements collected in this group are crucial for the generic IoT framework due to their fundamental roles in ensuring the effectiveness, reliability, and security of the entire system with BACS and IoT nodes. They are divided into six levels.

Device layer: sensors and actuators form the foundation of the field level within the network, enabling data collection and control, which are essential for smart decision-making both in building automation and smart homes. All international BACS standards, other standardized protocols (e.g., message queuing telemetry transport—MQTT, constrained application protocol—CoAP), and wireless-communication technologies discussed in Sections 1–3 should be considered for implementation at this layer.

Communication layer: standardized protocols and gateways facilitate seamless communication between diverse devices, providing interoperability and efficient data exchange. They should be considered for all network layers discussed in Section 2, implementing again the MQTT, CoAP, and additional real-time technologies and protocols.

Data-processing layer: Edge computing enhances real-time data processing near the device level within a local network, reducing latency and ensuring timely responses, while data filtering and aggregation optimize network resources. Considering fog computing and even integration with cloud computing, it is recommended to conduct research and development work with Amazon Web Services (AWS) IoT Greengrass, Google Cloud IoT Edge, and Azure IoT Edge.

Integration layer: BIM and DT based on the TCP/IP protocol and middleware enable the harmonious integration of IoT devices with building structures and diverse systems, promoting a cohesive and interoperable environment. It is suggested to conduct research and development work considering RESTful Application programming interfaces (APIs), MQTT, CoAP, etc., tools and protocols to develop standardized APIs and middleware to enable communication and data exchange between different IoT devices and systems, ensuring interoperability. An exploration of new service discovery algorithms should be mentioned as well. Their development and implementation would support the dynamic discovery and registration of IoT services and resources, facilitating the integration of new devices without manual configuration.

Security layer: end-to-end encryption and access controls are paramount for safeguarding sensitive data, ensuring the integrity and confidentiality of information in the BACS and BMS IoT ecosystem. Considering the openness of the IoT networks, developments of this layer should be considered first of all Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) aimed to identify and respond to potential security threats, enhancing the resilience of the IoT ecosystem. Moreover, implementation of end-to-end encryption with, for example, Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), should be examined, to secure data communication between IoT devices and the cloud, preventing unauthorized access and ensuring data confidentiality.

Cloud-computing layer: leveraging cloud storage and ensuring scalability supports the archiving of historical data and large-scale analytics and accommodates the evolving nature of generic IoT systems. There are many cloud services and tools that could be developed for this type of application, for example, AWS Lambda, Microsoft Azure Virtual Machines, Google Cloud Firestore, etc., with the aim to host applications and services that require computing resources, facilitate data processing, and application deployment.

It should be noted that these mandatory elements collectively establish a solid foundation for a reliable, secure, and integrated generic IoT framework. They address the core aspects of device communication, data processing, integration, and security, providing solutions for the successful implementation of advanced features and technologies in smart home and building applications with integrated IoT technologies.

5.2. Optional Elements of the Framework

The elements collected in this group enhance the generic IoT framework by introducing advanced capabilities that address the specific requirements of smart home and building applications and the overall performance of the generic IoT network. Considering that, they are presented in two subgroups, related to the smart home and the smart building.

5.2.1. Smart-Home Applications

Remote access and control: the development of mobile applications to provide homeowners and users with remote access to monitor and control smart-home devices; the implementation and integration of voice commands for convenient hands-free control. This application area is important for low-energy wireless-communication technologies such as BLE, ZigBee, and Z-Wave.

User interface: dashboards and control panels enable intuitive interfaces for homeowners to monitor and control smart-home devices effortlessly; moreover, customization of the user interfaces allows them to personalize automation rules based on their preferences, enhancing the user experience. In this field, several technical concepts could be considered for research and development, like voice command integration, with, for example, Amazon Alexa Skills Kit, Google Actions, etc. Moreover, web and mobile app development frameworks should be utilized to build responsive and interactive user interfaces for smart-home applications accessible through web browsers and mobile devices. Augmented reality will probably also be a new and emerging trend in organizing modern user interfaces.

Energy efficiency: integration of energy monitoring devices to empower homeowners with insights into energy consumption, promoting energy-efficient practices; smart grid integration explores connections with smart grids for optimized energy management within the smart-home environment, using DSM and DSR functions and tools. The most important directions of technological and systemic development seem to be (i) smart energy meters and IoT-enabled power outlets, allowing for the integration of energy monitoring devices to track and analyze the energy consumption of individual devices and appliances within the smart home; (ii) integration with local smart grids in relation to RES and energy storage use to optimize energy consumption, leveraging real-time data to make informed decisions about energy usage; and, last but not least, (iii) integration with dynamic pricing platforms (transactive energy mechanisms) implementing systems that adjust energy consumption based on dynamic pricing models, allowing users to optimize energy usage during periods of lower electricity costs.

5.2.2. Smart-Building Applications

Fog computing: local data-processing nodes deploying *fog computing* for smart-building applications, supporting local data processing for reduced latency and enhanced responsiveness in large-scale systems. Considering the fog computing layer/element, various tools and solutions can be employed to enhance real-time processing capabilities at the edge of the network. However, research and development are primarily suggested in the areas like leverage edge computing platforms (e.g., AWS IoT Greengrass, Azure IoT Edge, and Google Cloud IoT Edge) to extend cloud capabilities to edge devices, enabling local computation, data storage, and execution of IoT applications as well as the development of lightweight algorithms optimized for edge computing that are resource-efficient and well-suited for edge devices to enable real-time processing without compromising performance. Containerization is also an important emerging element that appears in the analyzed concepts for the development of fog computing for smart buildings. It provides tools to package and deploy applications consistently across edge devices, facilitating efficient deployment and management of fog computing resources.

ML and AI: utilizing ML for predictive analytics in smart-building management, optimizing resource allocation and improving overall efficiency and implementing of AI-based anomaly detection for proactive identification of faults and irregularities in building automation systems. Currently, it is a very dynamically developing field. The suggested main directions of research and development of ML and AI applications in smart building applications are (i) predictive maintenance models with ML algorithms that predict when building equipment and systems require maintenance, minimizing downtime and reducing operational costs; (ii) energy-consumption forecasting employing AI models to forecast building energy consumption, enabling proactive energy management and cost optimization with DSM and DSR mechanisms; and (iii) exploring of reinforcement learning techniques for building automation, allowing BACS and BMS systems to adapt and learn optimal control strategies over time.

Regulatory Compliance: ensure robust data-privacy measures to comply with regulations, addressing the unique challenges associated with handling sensitive data in smart-building applications and compliance with energy-efficiency standards where specific energy-efficiency standards applicable to commercial and large-scale buildings must be complied with. This area depends largely on institutions and nontechnical conditions. But, first of all, new regulations are expected in the field of data privacy, with a focus on protecting the personal information collected by smart-building systems, and updates to cybersecurity standards for IoT and smart buildings to address evolving threats and vulnerabilities. Moreover, establishing interoperability standards for smart buildings, ensuring compatibility and seamless integration of diverse devices and systems should be considered as well. In this context, regulations and standards for new smart-city platforms and frameworks are expected to promote the cohesive development of smart homes, buildings, and microgrids and the deployment of IoT technologies in these applications.

It should be noted that all elements from both subgroups can be mixed, being used in both smart home and building applications. However, he points out that some of them are dedicated only to specific applications, for example, regulatory compliance is specific to larger buildings.

5.3. SWOT Analysis and Discussion—Main Challenges, Opportunities, Pros, and Cons

The usefulness of the presented generic IoT framework requires an analysis of the possibilities and challenges arising from its potential implementation and possible difficulties as well as threats in its practical implementation in a smart home and BACS and BMS with IoT installations. Therefore, the author decided to present the SWOT analysis, along with a short discussion.

S—Strengths:

- Comprehensive integration: the incorporation of mandatory elements from the framework ensures a solid foundation for seamless device communication, data processing, and security;
- Flexibility and scalability: the inclusion of optional elements allows for customization based on specific applications, catering to the unique needs of both smart homes and buildings;
- Advanced capabilities: optional elements such as fog computing, machine learning, and AI enhance the framework's capabilities, providing predictive analytics, anomaly detection, and efficient resource management.

W—Weaknesses:

- Complex implementation: the inclusion of various optional elements may introduce complexity in the implementation phase, requiring careful planning and expertise;
- Resource intensiveness: certain advanced features, such as ML and AI, may demand substantial computing resources, potentially affecting system performance;
- Potential security risks: the complexity of the framework may introduce vulnerabilities, necessitating robust cybersecurity measures to mitigate potential risks.

O—Opportunities:

- Market growth: the rising demand for smart home and building solutions, as well as IoT and TIoT, presents a significant market opportunity, with the framework well-positioned to capitalize on this trend;
- Technological advancements: ongoing advancements in IoT technologies, including edge, fog computing, ML and AI offer opportunities for continuous improvement and innovation within the framework;
- Regulatory support: compliance with emerging data-privacy and energy-efficiency regulations can enhance the credibility of the framework and market acceptance.

T—Threats:

- Cybersecurity concerns: as IoT systems become more interconnected, the framework faces potential threats from cyberattacks, necessitating robust security measures;
- Integration challenges: compatibility issues with existing systems in buildings or homes may pose challenges during implementation, requiring seamless integration strategies;

- Market, research, and technical competition: rapid technological advancements may lead to increased competition, requiring continuous updates to maintain the framework's competitiveness.

The generic IoT framework for smart home and building applications proposed in this paper is a comprehensive solution with strengths in integration, flexibility, and advanced functional capabilities. The latter, in particular, requires consideration when implemented in smart-home applications. The underlying integration of BACS and BMS techniques with the IoT poses challenges, including the potential complexity of implementation, the intensity of use of resources available in the network node modules, and data security threats. Therefore, the successful implementation of the generic IoT platform based on the presented framework depends on the effective management of system complexity, tracking technological trends, and solving security and compatibility issues in order to meet the changing needs of the smart home and building industry.

What is very important and significant is to address the weaknesses and threats identified in the SWOT analysis for generic IoT in smart home and building applications; the following research and development directions can be proposed:

Reducing weaknesses

1. Simplify implementation processes by developing automated deployment tools and standardized templates to simplify the installation and configuration of IoT devices in smart homes and buildings. Automation and standardization can minimize the complexity of implementation, making it more user-friendly and reducing the potential for errors;
2. Resource optimization for advanced functions by exploring lightweight algorithms and edge computing strategies to optimize resource-intensive functions, such as machine learning and AI, to ensure efficient operation in resource-constrained environments. Optimizing resources reduces the load on devices and networks, improving overall system performance;
3. Enhance cybersecurity measures by exploring blockchain-based security frameworks, decentralized identity management, and real-time threat detection to strengthen the security posture of smart home and building IoT systems. Implementing advanced cybersecurity measures will strengthen defenses against evolving threats, protect sensitive data, and ensure the integrity of the system.

Mitigating threats

1. Enhance cybersecurity awareness and education by conducting research on effective cybersecurity awareness and education programs for both users and developers involved in IoT applications for smart homes and buildings. Increased awareness and education can empower users to adopt secure practices, reducing the risk of cyber threats such as unauthorized access or data breaches;
2. Standardize security protocols by working with industry stakeholders to establish and promote standardized security protocols for IoT devices and communications in smart home and building ecosystems. Standardization ensures a consistent and robust security framework, making it harder for attackers to exploit vulnerabilities;
3. Continuous monitoring and updating by researching dynamic monitoring solutions and automated update mechanisms to ensure continuous monitoring of IoT systems and rapid deployment of security patches. Proactive monitoring and timely updates reduce the vulnerability window, mitigating potential threats to the IoT ecosystem;
4. Interoperability testing by developing comprehensive interoperability testing frameworks to verify the compatibility of IoT devices with different platforms and protocols. Ensuring interoperability reduces the likelihood

of integration challenges and enhances the overall reliability of smart home and building IoT systems.

6. Conclusions

IoT technologies set the direction for the development of many industries related to IT and automation. In particular, in line with the concept of distributed system architecture, they are increasingly entering the structures of BACS networks in smart home and building applications. Along with this process, the technological and functional complexity of these types of systems increases. This paper provides a systematic literature review of the state-of-the-art development of several aspects related to the development of modern smart home and building platforms. The author traced the path of changes in the architecture of distributed automation systems, with an analysis of new edge and fog computing paradigms, implemented at the level of local BACS networks, BMS with IoT modules, and TCP/IP communication channels. Then, application areas for big-data-processing technologies and the implementation of advanced ML and AI techniques supporting the implementation of control functions and effective management of the infrastructure of houses and buildings were identified and discussed. Finally, there is proposed the framework structure for a generic IoT dedicated to applications in building automation in elements of Internet services and local automation servers. A SWOT analysis was performed for the proposed framework in the context of the potential use of BACS network systems with IoT elements in smart home and building applications.

Future research and development work in the generic IoT concept for smart home and building applications could explore enhancing interoperability through standardized communication protocols for seamless integration with a diverse range of devices, for example within platforms like Home Assistant. Moreover, investigating ML applications within Home Assistant and other similar tools can further optimize automation rules, offering personalized and context-aware user experiences. Additionally, exploring energy-efficient algorithms and predictive analytics within the proposed framework could contribute to resource-management efforts and improve overall sustainability in smart homes and buildings.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
API	Application Programming Interface
AWS	Amazon Web Services
BaaS	Building as a Service
BACS	Building Automation and Control Systems
BIM	Building Information Modeling
BLE	Bluetooth Low Energy
BMS	Building Management Systems
CoAP	Constrained Application Protocol
DoS	Denial-of-Service
DSM	Demand Side Management
DSR	Demand Side Response
DT	Digital Twin
DTLS	Datagram Transport Layer Security
EPBD	Energy Performance of Buildings Directive
FL	Federated Learning

FM	Facility Management
FoE	Fog of Everything
HVAC	Heating, Ventilation, Air Conditioning
ICT-	Information and Communications Technology
IDS	Intrusion Detection Systems
IoE	Internet of Everything
IoT	Internet of Things
IOTA	Internet of Things Application
IPS	Intrusion Prevention Systems (IPS)
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport protocol
OPC	OLE for Process Control (OLE—Object Linking and Embedding)
P2P	Peer-to-Peer
PLC-	Programmable Logic Controller
RES-	Renewable Energy Sources
SoC-	System-on-a-Chip
SRI-	Smart Readiness Indicator
TIoT	Tactile Internet of Things
TLS	Transport Layer Security
WoT	Web of Things

References

1. Benotmane, M.; Elhari, K.; Kabbaj, A. A Review & Analysis of Current IoT Maturity & Readiness Models and Novel Proposal. *Sci. Afr.* **2023**, *21*, e01748. https://doi.org/10.1016/j.sciaf.2023.e01748.
2. Khattak, S.B.A.; Nasralla, M.M.; Farman, H.; Choudhury, N. Performance Evaluation of an IEEE 802.15.4-Based Thread Network for Efficient Internet of Things Communications in Smart Cities. *Appl. Sci.* **2023**, *13*, 7745. https://doi.org/10.3390/app13137745.
3. Ferrández-Pastor, F.-J.; Mora, H.; Jimeno-Morenilla, A.; Volckaert, B. Deployment of IoT Edge and Fog Computing Technologies to Develop Smart Building Services. *Sustainability* **2018**, *10*, 3832. https://doi.org/10.3390/su10113832.
4. Ali, O.; Ishak, M.K. Bringing Intelligence to IoT Edge: Machine Learning Based Smart City Image Classification Using Microsoft Azure IoT and Custom Vision. *J. Phys. Conf. Ser.* **2020**, *1529*, 042076. https://doi.org/10.1088/1742-6596/1529/4/042076.
5. 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.
6. Sharma, H.; Haque, A.; Blaabjerg, F. Machine Learning in Wireless Sensor Networks for Smart Cities: A Survey. *Electronics* **2021**, *10*, 1012. https://doi.org/10.3390/electronics10091012.
7. Wang, B.; Li, M.; Jin, X.; Guo, C. A Reliable IoT Edge Computing Trust Management Mechanism for Smart Cities. *IEEE Access* **2020**, *8*, 46373–46399. https://doi.org/10.1109/ACCESS.2020.2979022.
8. *ISO/IEC 14543-3-10:2020*; Information Technology Home Electronic Systems (HES) Architecture—KNX. International Organization for Standardization: Geneva, Switzerland, 2020.
9. *ISO/IEC 14908-1:2012*; Information Technology Control Network Protocol—LonWorks. International Organization for Standardization: Geneva, Switzerland, 2012.
10. *ISO 16484-6:2020*; Building Automation and Control Systems (BACS)—BACnet. International Organization for Standardization: Geneva, Switzerland, 2020.
11. Bovet, G.; Hennebert, J. Will Web Technologies Impact on Building Automation Systems Architecture? *Procedia Comput. Sci.* **2014**, *32*, 985–990. https://doi.org/10.1016/j.procs.2014.05.522.
12. Ożadowicz, A. A New Concept of Active Demand Side Management for Energy Efficient Prosumer Microgrids with Smart Building Technologies. *Energies* **2017**, *10*, 1771. https://doi.org/10.3390/en10111771.
13. Schraven, M.H.; Droste, K.; Guarnieri Calò Carducci, C.G.C.; Müller, D.; Monti, A. Open-Source Internet of Things Gateways for Building Automation Applications. *J. Sens. Actuator Netw.* **2022**, *11*, 74. https://doi.org/10.3390/jsan11040074.
14. Froiz-Míguez, I.; Fernández-Caramés, T.; Fraga-Lamas, P.; Castedo, L. Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes. *Sensors* **2018**, *18*, 2660. https://doi.org/10.3390/s18082660.
15. Petkov, N.; Naumov, A. Overview of Industrial Communication in Process Automation. In Proceedings of the 2022 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 6–8 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 229–234.
16. Secgin, S. Seven Layers of ISO/OSI. In *Evolution of Wireless Communication Ecosystems*; Wiley: Hoboken, NJ, USA, 2023; pp. 41–50.
17. Vernadat, F.B. Interoperability and Standards for Automation. In *Springer Handbook of Automation*; Nof, S.Y., Ed.; Springer International Publishing: Cham, Switzerland, 2023; pp. 729–752.

18. Kato, T.; Ishikawa, N.; Yoshida, N. Distributed Autonomous Control of Home Appliances Based on Event Driven Architecture. In Proceedings of the 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya, Japan, 24–27 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–2.
19. Graveto, V.; Cruz, T.; Simöes, P. Security of Building Automation and Control Systems: Survey and Future Research Directions. *Comput. Secur.* **2022**, *112*, 102527. https://doi.org/10.1016/j.cose.2021.102527.
20. Martirano, L.; Mitolo, M. Building Automation and Control Systems (BACS): A Review. In Proceedings of the 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Madrid, Spain, 9–12 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–8.
21. Ożadowicz, A.; Grela, J. An Event-Driven Building Energy Management System Enabling Active Demand Side Management. In Proceedings of the 2016 Second International Conference on Event-based Control, Communication, and Signal Processing (EBCCSP), Krakow, Poland, 13–15 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–8.
22. Pirbhulal, S.; Zhang, H.; E Alahi, M.; Ghayvat, H.; Mukhopadhyay, S.; Zhang, Y.-T.; Wu, W. A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network. *Sensors* **2016**, *17*, 69. https://doi.org/10.3390/s17010069.
23. Ożadowicz, A. Technical, Qualitative and Energy Analysis of Wireless Control Modules for Distributed Smart Home Systems. *Future Internet* **2023**, *15*, 316. https://doi.org/10.3390/fi15090316.
24. Prakosa, S.; Nugraha, A.; Atiq, M. Miniature SmartHome Dengan Sonoff. *J. Ris. Rumpun Ilmu Tek.* **2023**, *2*, 41–55.
25. Yang, H.; Kim, B.; Lee, J.; Ahn, Y.; Lee, C. Advanced Wireless Sensor Networks for Sustainable Buildings Using Building Ducts. *Sustainability* **2018**, *10*, 2628. https://doi.org/10.3390/su10082628.
26. Anush, K.S.; Sasikala, S.; Arun, K.S.; Arunan, R.; Asfaq, M.A. Enhanced and Secured Smart Home Using Z-Wave Technology. In Proceedings of the 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation, ICAECA 2023, Coimbatore, India, 16–17 June 2023; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2023.
27. Kazeem, O.O.; Akintade, O.; Kehinde, L.O.; Akintade, O.O.; Kehinde, L.O. Comparative Study of Communication Interfaces for Sensors and Actuators in the Cloud of Internet of Things. *Int. J. Internet Things* **2017**, *2017*, 9–13. https://doi.org/10.5923/j.ijit.20170601.02.
28. Wang, J. Zigbee Light Link and Its Applicationss. *IEEE Wirel. Commun.* **2013**, *20*, 6–7. https://doi.org/10.1109/MWC.2013.6590043.
29. Rohini, S.; Venkatasubramanian, K. Z-Wave Based Zoning Sensor for Smart Thermostats. *Indian J. Sci. Technol.* **2015**, *8, 1-6*. https://doi.org/10.17485/ijst/2015/v8i20/79081.
30. Ali, A.I.; Partal, S.Z.; Kepke, S.; Partal, H.P. ZigBee and LoRa Based Wireless Sensors for Smart Environment and IoT Applications. In Proceedings of the 2019 1st Global Power, Energy and Communication Conference (GPECOM), Nevsehir, Turkey, 12–15 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 19–23.
31. 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; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
32. Filippoupolitis, A.; Oliff, W.; Loukas, G. Bluetooth Low Energy Based Occupancy Detection for Emergency Management. In Proceedings of the 2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS), Granada, Spain, 14–16 December 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 31–38.
33. Zhuang, Y.; Yang, J.; Li, Y.; Qi, L.; El-Sheimy, N. Smartphone-Based Indoor Localization with Bluetooth Low Energy Beacons. *Sensors* **2016**, *16*, 596. https://doi.org/10.3390/s16050596.
34. Collotta, M.; Pau, G. A Solution Based on Bluetooth Low Energy for Smart Home Energy Management. *Energies* **2015**, *8*, 11916–11938. https://doi.org/10.3390/en81011916.
35. Tekler, Z.D.; Low, R.; Yuen, C.; Blessing, L. Plug-Mate: An IoT-Based Occupancy-Driven Plug Load Management System in Smart Buildings. *Build. Environ.* **2022**, *223*, 109472. https://doi.org/10.1016/j.buildenv.2022.109472.
36. Balaji, B.; Xu, J.; Nwokafor, A.; Gupta, R.; Agarwal, Y. Sentinel: Occupancy Based HVAC Actuation Using Existing WiFi Infrastructure within Commercial Buildings. In Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems, Roma, Italy, 11–15 November 2013; ACM: New York, NY, USA, 2013; pp. 1–14.
37. Tekler, Z.D.; Lei, Y.; Dai, X.; Chong, A. Enhancing Personalised Thermal Comfort Models with Active Learning for Improved HVAC Controls. *J. Phys. Conf. Ser.* **2023**, *2600*, 132004. https://doi.org/10.1088/1742-6596/2600/13/132004.
38. Singhai, R.; Sushil, R. An Investigation of Various Security and Privacy Issues in Internet of Things. *Mater. Today Proc.* **2023**, *80*, 3393–3397. https://doi.org/10.1016/j.matpr.2021.07.259.
39. Nasir, M.; Muhammad, K.; Ullah, A.; Ahmad, J.; Wook Baik, S.; Sajjad, M. Enabling Automation and Edge Intelligence over Resource Constraint IoT Devices for Smart Home. *Neurocomputing* **2022**, *491*, 494–506. https://doi.org/10.1016/j.neucom.2021.04.138.
40. Lăcătușu, F.; Ionita, A.D.; Lăcătușu, M.; Olteanu, A. Performance Evaluation of Information Gathering from Edge Devices in a Complex of Smart Buildings. *Sensors* **2022**, *22*, 1002. https://doi.org/10.3390/s22031002.
41. Babar, M.; Grela, J.; Ożadowicz, A.; Nguyen, P.; Hanzelka, Z.; Kamphuis, I. Energy Flexometer: Transactive Energy-Based Internet of Things Technology. *Energies* **2018**, *11*, 568. https://doi.org/10.3390/en11030568.
42. Faqiry, M.; Edmonds, L.; Zhang, H.; Khodaei, A.; Wu, H. Transactive-Market-Based Operation of Distributed Electrical Energy Storage with Grid Constraints. *Energies* **2017**, *10*, 1891. https://doi.org/10.3390/en10111891.

43. Pratt, A.; Krishnamurthy, D.; Ruth, M.; Wu, H.; Lunacek, M.; Vaynshenk, P. Transactive Home Energy Management Systems: The Impact of Their Proliferation on the Electric Grid. *IEEE Electrif. Mag.* **2016**, *4*, 8–14. https://doi.org/10.1109/MELE.2016.2614188.
44. Ożadowicz, A. A Hybrid Approach in Design of Building Energy Management System with Smart Readiness Indicator and Building as a Service Concept. *Energies* **2022**, *15*, 1432. https://doi.org/10.3390/en15041432.
45. Laroui, M.; Nour, B.; Moungla, H.; Cherif, M.A.; Afifi, H.; Guizani, M. Edge and Fog Computing for IoT: A Survey on Current Research Activities & Future Directions. *Comput. Commun.* **2021**, *180*, 210–231. https://doi.org/10.1016/j.comcom.2021.09.003.
46. Yousefpour, A.; Fung, C.; Nguyen, T.; Kadiyala, K.; Jalali, F.; Niakanlahiji, A.; Kong, J.; Jue, J.P. All One Needs to Know about Fog Computing and Related Edge Computing Paradigms: A Complete Survey. *J. Syst. Archit.* **2019**, *98*, 289–330. https://doi.org/10.1016/j.sysarc.2019.02.009.
47. Huang, Z.; Lin, K.-J.; Tsai, B.-L.; Yan, S.; Shih, C.-S. Building Edge Intelligence for Online Activity Recognition in Service-Oriented IoT Systems. *Future Gener. Comput. Syst.* **2018**, *87*, 557–567. https://doi.org/10.1016/j.future.2018.03.003.
48. Filho, G.P.R.; Meneguette, R.I.; Maia, G.; Pessin, G.; Gonçalves, V.P.; Weigang, L.; Ueyama, J.; Villas, L.A. A Fog-Enabled Smart Home Solution for Decision-Making Using Smart Objects. *Future Gener. Comput. Syst.* **2020**, *103*, 18–27. https://doi.org/10.1016/j.future.2019.09.045.
49. Mahmud, R.; Kotagiri, R.; Buyya, R. Fog Computing: A Taxonomy, Survey and Future Directions. In *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*; Di Martino, B., Li, K.-C., Yang, L., Esposito, A., Eds.; Springer: Singapore, 2018; pp. 103–130.
50. Alnajar, O.; Barnawi, A. Tactile Internet of Federated Things: Toward Fine-Grained Design of FL-Based Architecture to Meet TIoT Demands. *Comput. Netw.* **2023**, *231*, 109712. https://doi.org/10.1016/j.comnet.2023.109712.
51. Sun, H.; Yu, H.; Fan, G.; Chen, L. Energy and Time Efficient Task Offloading and Resource Allocation on the Generic IoT-Fog-Cloud Architecture. *Peer Peer Netw. Appl.* **2020**, *13*, 548–563. https://doi.org/10.1007/s12083-019-00783-7.
52. Li, W.; Wang, S. A Fully Distributed Optimal Control Approach for Multi-Zone Dedicated Outdoor Air Systems to Be Implemented in IoT-Enabled Building Automation Networks. *Appl. Energy* **2022**, *308*, 118408. https://doi.org/10.1016/j.apenergy.2021.118408.
53. Ge, X.; Yang, F.; Han, Q. Distributed Networked Control Systems: A Brief Overview. *Inf. Sci.* **2017**, *380*, 117–131. https://doi.org/10.1016/j.ins.2015.07.047.
54. Islam, R.; Rahman, M.W.; Rubaiat, R.; Hasan, M.M.; Reza, M.M.; Rahman, M.M. LoRa and Server-Based Home Automation Using the Internet of Things (IoT). *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 3703–3712. https://doi.org/10.1016/j.jksuci.2020.12.020.
55. Bhatt, J.; Verma, H.K. Design and Development of Wired Building Automation Systems. *Energy Build.* **2015**, *103*, 396–413. https://doi.org/10.1016/j.enbuild.2015.02.054.
56. Merz, H.; Hansemann, T.; Hübner, C. *Building Automation*; Signals and Communication Technology; Springer International Publishing: Cham, Switzerland, 2018; ISBN 978-3-319-73222-0.
57. Dietrich, D.; Bruckner, D.; Zucker, G.; Palensky, P. Communication and Computation in Buildings: A Short Introduction and Overview. *IEEE Trans. Ind. Electron.* **2010**, *57*, 3577–3584. https://doi.org/10.1109/TIE.2010.2046570.
58. Wang, S. *Intelligent Buildings and Building Automation*; Routledge: London, UK, 2009; ISBN 9781134025107.
59. Domingues, P.; Carreira, P.; Vieira, R.; Kastner, W. Building Automation Systems: Concepts and Technology Review. *Comput. Stand. Interfaces* **2016**, *45*, 1–12. https://doi.org/10.1016/j.csi.2015.11.005.
60. Lobaccaro, G.; Carlucci, S.; Löfström, E. A Review of Systems and Technologies for Smart Homes and Smart Grids. *Energies* **2016**, *9*, 348. https://doi.org/10.3390/en9050348.
61. NORDIC Semiconductor Nordic Semiconductor Delivers Industry-Wide Support for KNX IoT Protocol Following Membership of KNX Association. Available online: https://www.nordicsemi.com/Nordic-news/2023/06/nordic-delivers-industry-wide-support-for-knx-iot-protocol-following-membership-of-knx-association (accessed on 8 December 2023).
62. HAGER Connecting the World of Digital Objects and Services with KNX. Available online: https://assets1.sc.hager.com/turkey/files/IoT-Controller.pdf (accessed on 8 December 2023).
63. EXOR Powerful IoT-Ready Interfaces with KNX Interface. Available online: https://www.exorint.com/corporate/press-release/knx-2020 (accessed on 8 December 2023).
64. Kortuem, G.; Kawsar, F.; Sundramoorthy, V.; Fitton, D. Smart Objects as Building Blocks for the Internet of Things. *IEEE Internet Comput.* **2010**, *14*, 44–51. https://doi.org/10.1109/MIC.2009.143.
65. Bin, S.; Guiqing, Z.; Shaolin, W.; Dong, W. The Development of Management System for Building Equipment Internet of Things. In Proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, 27–29 May 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 423–427.
66. Jarvinen, H.; Litvinov, A.; Vuorimaa, P. Integration Platform for Home and Building Automation Systems. In Proceedings of the 2011 IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 292–296.
67. Jung, M.; Reinisch, C.; Kastner, W. Integrating Building Automation Systems and IPv6 in the Internet of Things. In Proceedings of the 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Palermo, Italy, 4–6 July 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 683–688.

68. 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. https://doi.org/10.1016/j.scs.2016.08.019.
69. Lilis, G.; Conus, G.; Kayal, M. A Distributed, Event-Driven Building Management Platform on Web Technologies. In Proceedings of the 2015 International Conference on Event-based Control, Communication, and Signal Processing (EBCCSP), Krakow, Poland, 17–19 June 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–8.
70. Conus, G.; Lilis, G.; Zanjani, N.A.; Kayal, M. Toward Event-Driven Mechanism for Load Profile Generation. In Proceedings of the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 12–15 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
71. Mansour, M.; Gamal, A.; Ahmed, A.I.; Said, L.A.; Elbaz, A.; Herencsar, N.; Soltan, A. Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. *Energies* **2023**, *16*, 3465. https://doi.org/10.3390/en16083465.
72. Ramprasad, B.; McArthur, J.; Fokaefs, M.; Barna, C.; Damm, M.; Litoiu, M. Leveraging Existing Sensor Networks as IoT Devices for Smart Buildings. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 452–457.
73. Vicari, N.; Wuchner, E.; Broring, A.; Niedermeier, C. Engineering and operation made easy - a semantics and service-oriented approach to building automation. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8-11 September 2015; pp. 1–8. https://doi.org/10.1109/ETFA.2015.7301657.
74. Baccarelli, E.; Naranjo, P.G.V.; Scarpiniti, M.; Shojafar, M.; Abawajy, J.H. Fog of Everything: Energy-Efficient Networked Computing Architectures, Research Challenges, and a Case Study. *IEEE Access* **2017**, *5*, 9882–9910. https://doi.org/10.1109/ACCESS.2017.2702013.
75. Wildenauer, A.; Mbabu, A.; Underwood, J.; Basl, J. Building-as-a-Service: Theoretical Foundations and Conceptual Framework. *Buildings* **2022**, *12*, 1594. https://doi.org/10.3390/buildings12101594.
76. Wildenauer, A.; Basl, J. Building-as-a-Service: The Opportunities of Service-Dominant Logic for Construction. *Mark. Sci. Inspir.* **2022**, *17*, 41–53. https://doi.org/10.46286/msi.2022.17.3.5.
77. *European Parliament Directive (EU) 2018/844 of the European Parliament and the Council on the Energy Performance of Buildings*; EU: 2018, Strasbourg, France.
78. Verbeke, S.; Aerts, D.; Reynders, G.; Ma, Y.; Waide, P. *Final Report on the Technical Support to the Development of a Smart Readiness Indicator for Buildings*; European Commission: Brussels, Belgium, 2020.
79. Ramezani, B.; da Silva, M.G.; Simões, N. Application of Smart Readiness Indicator for Mediterranean Buildings in Retrofitting Actions. *Energy Build.* **2021**, *249*, 111173. https://doi.org/10.1016/j.enbuild.2021.111173.
80. Mancini, F.; Lo Basso, G.; de Santoli, L. Energy Use in Residential Buildings: Impact of Building Automation Control Systems on Energy Performance and Flexibility. *Energies* **2019**, *12*, 2896. https://doi.org/10.3390/en12152896.
81. Fokaides, P.A.; Panteli, C.; Panayidou, A. How Are the Smart Readiness Indicators Expected to Affect the Energy Performance of Buildings: First Evidence and Perspectives. *Sustainability* **2020**, *12*, 9496. https://doi.org/10.3390/su12229496.
82. Vasilopoulos, V.G.; Dimara, A.; Krinidis, S.; Almpanis, P.; Margaritis, N.; Nikolopoulos, N.; Ioannidis, D.; Tzovaras, D. An IoT M2M Architecture for BMS Using Multiple Connectivity Technologies: A Practical Approach. In Proceedings of the 2021 6th International Conference on Smart and Sustainable Technologies (SpliTech), Bol and Split, Croatia, 8–11 September 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
83. Fetahi, E.; Ajdari, J.; Zenuni, X.; Hamiti, M. A Cloud Centric Smart City Construction with an IoT Enabled Traffic Prediction Mechanism. In Proceedings of the 2022 11th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 7–10 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
84. Chen, Y.-C.; Chang, Y.-C.; Chen, C.-H.; Lin, Y.-S.; Chen, J.-L.; Chang, Y.-Y. Cloud-Fog Computing for Information-Centric Internet-of-Things Applications. In Proceedings of the 2017 International Conference on Applied System Innovation (ICASI), Sapporo, Japan, 13–17 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 637–640.
85. Sahil; Sood, S.K. Fog-Cloud Centric IoT-Based Cyber Physical Framework for Panic Oriented Disaster Evacuation in Smart Cities. *Earth Sci. Inform.* **2022**, *15*, 1449–1470. https://doi.org/10.1007/s12145-020-00481-6.
86. NVIDIA Developer Jetson Nano Developer Kit. Available online: https://developer.nvidia.com/embedded/jetson-nano-developer-kit (accessed on 14 December 2023).
87. Yar, H.; Imran, A.S.; Khan, Z.A.; Sajjad, M.; Kastrati, Z. Towards Smart Home Automation Using IoT-Enabled Edge-Computing Paradigm. *Sensors* **2021**, *21*, 4932. https://doi.org/10.3390/s21144932.
88. Alshaikhli, M.; Elfouly, T.; Elharrouss, O.; Mohamed, A.; Ottakath, N. Evolution of Internet of Things From Blockchain to IOTA: A Survey. *IEEE Access* **2022**, *10*, 844–866. https://doi.org/10.1109/ACCESS.2021.3138353.
89. Parikh, S.; Dave, D.; Patel, R.; Doshi, N. Security and Privacy Issues in Cloud, Fog and Edge Computing. *Procedia Comput. Sci.* **2019**, *160*, 734–739. https://doi.org/10.1016/j.procs.2019.11.018.
90. Alwakeel, A.M. An Overview of Fog Computing and Edge Computing Security and Privacy Issues. *Sensors* **2021**, *21*, 8226. https://doi.org/10.3390/s21248226.
91. Ullah, A.; Ullah, S.I.; Salam, A. Internal DoS Attack Detection and Prevention in Fog Computing. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 763–768.

92. Huso, I.; Piro, G.; Boggia, G. Distributed and Privacy-Preserving Data Dissemination at the Network Edge via Attribute-Based Searchable Encryption. In Proceedings of the 2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet), Pafos, Cyprus, 1–3 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 122–130.
93. Xu, R.; Palanisamy, B.; Joshi, J. QueryGuard: Privacy-Preserving Latency-Aware Query Optimization for Edge Computing. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1097–1106.
94. Alam, T. Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges. *Computers* **2022**, *12*, 6. https://doi.org/10.3390/computers12010006.
95. Taneja, S.; Rana, I.; Tyagi, S. Blockchain for Iot Security and Privacy: Smart Home-A Review. *Int. J. Adv. Eng. Manag.* **2023**, *5*, 1293. https://doi.org/10.35629/5252-050512931296.
96. Moniruzzaman, M.; Khezr, S.; Yassine, A.; Benlamri, R. Blockchain for Smart Homes: Review of Current Trends and Research Challenges. *Comput. Electr. Eng.* **2020**, *83*, 106585. https://doi.org/10.1016/j.compeleceng.2020.106585.
97. Afzal, M.; Huang, Q.; Amin, W.; Umer, K.; Raza, A.; Naeem, M. Blockchain Enabled Distributed Demand Side Management in Community Energy System With Smart Homes. *IEEE Access* **2020**, *8*, 37428–37439. https://doi.org/10.1109/ACCESS.2020.2975233.
98. Tyagi, A.K.; Dananjayan, S.; Agarwal, D.; Thariq Ahmed, H.F. Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. *Sensors* **2023**, *23*, 947. https://doi.org/10.3390/s23020947.
99. Arif, S.; Khan, M.A.; Rehman, S.U.; Kabir, M.A.; Imran, M. Investigating Smart Home Security: Is Blockchain the Answer? *IEEE Access* **2020**, *8*, 117802–117816. https://doi.org/10.1109/ACCESS.2020.3004662.
100. Abed, S.; Jaffal, R.; Mohd, B.J. A Review on Blockchain and IoT Integration from Energy, Security and Hardware Perspectives. *Wirel. Pers. Commun.* **2023**, *129*, 2079–2122. https://doi.org/10.1007/s11277-023-10226-5.
101. Djenouri, D.; Laidi, R.; Djenouri, Y.; Balasingham, I. Machine Learning for Smart Building Applications. *ACM Comput. Surv.* **2020**, *52*, 24. https://doi.org/10.1145/3311950.
102. Shayeghi, H.; Shahryari, E.; Moradzadeh, M.; Siano, P. A Survey on Microgrid Energy Management Considering Flexible Energy Sources. *Energies* **2019**, *12*, 2156. https://doi.org/10.3390/en12112156.
103. Hou, P.; Yang, G.; Hu, J.; Douglass, P.J.; Xue, Y. A Distributed Transactive Energy Mechanism for Integrating PV and Storage Prosumers in Market Operation. *Engineering* **2022**, *12*, 171–182. https://doi.org/10.1016/j.eng.2022.03.001.
104. Pipattanasomporn, M.; Kuzlu, M.; Rahman, S.; Teklu, Y. Load Profiles of Selected Major Household Appliances and Their Demand Response Opportunities. *IEEE Trans Smart Grid* **2014**, *5*, 742–750. https://doi.org/10.1109/TSG.2013.2268664.
105. Bouchabou, D.; Nguyen, S.M.; Lohr, C.; LeDuc, B.; Kanellos, I. A Survey of Human Activity Recognition in Smart Homes Based on IoT Sensors Algorithms: Taxonomies, Challenges, and Opportunities with Deep Learning. *Sensors* **2021**, *21*, 6037. https://doi.org/10.3390/s21186037.
106. Suman, S.; Etemad, A.; Rivest, F. Potential Impacts of Smart Homes on Human Behavior: A Reinforcement Learning Approach. *IEEE Trans. Artif. Intell.* **2022**, *3*, 567–580. https://doi.org/10.1109/TAI.2021.3127483.
107. Machorro-Cano, I.; Alor-Hernández, G.; Paredes-Valverde, M.A.; Rodríguez-Mazahua, L.; Sánchez-Cervantes, J.L.; Olmedo-Aguirre, J.O. HEMS-IoT: A Big Data and Machine Learning-Based Smart Home System for Energy Saving. *Energies* **2020**, *13*, 1097. https://doi.org/10.3390/en13051097.
108. Shah, S.; Iqbal, M.; Aziz, Z.; Rana, T.; Khalid, A.; Cheah, Y.-N.; Arif, M. The Role of Machine Learning and the Internet of Things in Smart Buildings for Energy Efficiency. *Appl. Sci.* **2022**, *12*, 7882. https://doi.org/10.3390/app12157882.
109. Kawa, B.; Borkowski, P. Integration of Machine Learning Solutions in the Building Automation System. *Energies* **2023**, *16*, 4504. https://doi.org/10.3390/en16114504.
110. Vassiliades, C.; Agathokleous, R.; Barone, G.; Forzano, C.; Giuzio, G.F.; Palombo, A.; Buonomano, A.; Kalogirou, S. Building Integration of Active Solar Energy Systems: A Review of Geometrical and Architectural Characteristics. *Renew. Sustain. Energy Rev.* **2022**, *164*, 112482. https://doi.org/10.1016/j.rser.2022.112482.
111. Fambri, G.; Badami, M.; Tsagkrasoulis, D.; Katsiki, V.; Giannakis, G.; Papanikolaou, A. Demand Flexibility Enabled by Virtual Energy Storage to Improve Renewable Energy Penetration. *Energies* **2020**, *13*, 5128. https://doi.org/10.3390/en13195128.
112. Cvitić, I.; Peraković, D.; Periša, M.; Gupta, B. Ensemble Machine Learning Approach for Classification of IoT Devices in Smart Home. *Int. J. Mach. Learn. Cybern.* **2021**, *12*, 3179–3202. https://doi.org/10.1007/s13042-020-01241-0.
113. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A Survey on Federated Learning. *Knowl.-Based Syst.* **2021**, *216*, 106775. https://doi.org/10.1016/j.knosys.2021.106775.
114. Mammen, P.M. Federated Learning: Opportunities and Challenges. *arXiv* **2021**, arXiv:2101.05428.
115. Zubaydi, H.D.; Varga, P.; Molnár, S. Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors* **2023**, *23*, 788.
116. Yazdinejad, A.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G.; Karimipour, H. Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. *Comput. Ind.* **2023**, *144*, 103801. https://doi.org/10.1016/j.compind.2022.103801.
117. Khan, M.A.; Abbas, S.; Rehman, A.; Saeed, Y.; Zeb, A.; Uddin, M.I.; Nasser, N.; Ali, A. A Machine Learning Approach for Blockchain-Based Smart Home Networks Security. *IEEE Netw.* **2021**, *35*, 223–229. https://doi.org/10.1109/MNET.011.2000514.
118. Panchalingam, R.; Chan, K.C. A State-of-the-Art Review on Artificial Intelligence for Smart Buildings. *Intell. Build. Int.* **2021**, *13*, 203–226. https://doi.org/10.1080/17508975.2019.1613219.

119. Rodriguez-Garcia, P.; Li, Y.; Lopez-Lopez, D.; Juan, A.A. Strategic Decision Making in Smart Home Ecosystems: A Review on the Use of Artificial Intelligence and Internet of Things. *Internet Things* **2023**, *22*, 100772. https://doi.org/10.1016/j.iot.2023.100772.
120. Genkin, M.; McArthur, J.J. B-SMART: A Reference Architecture for Artificially Intelligent Autonomic Smart Buildings. *Eng. Appl. Artif. Intell.* **2023**, *121*, 106063. https://doi.org/10.1016/j.engappai.2023.106063.
121. Hou, Z.; She, C.; Li, Y.; Niyato, D.; Dohler, M.; Vucetic, B. Intelligent Communications for Tactile Internet in 6G: Requirements, Technologies, and Challenges. *IEEE Commun. Mag.* **2021**, *59*, 82–88. https://doi.org/10.1109/MCOM.006.2100227.
122. Fanibhare, V.; Sarkar, N.I.; Al-Anbuky, A. A Survey of the Tactile Internet: Design Issues and Challenges, Applications, and Future Directions. *Electronics* **2021**, *10*, 2171. https://doi.org/10.3390/electronics10172171.
123. Akshatha, N.; Rai, K.H.; Haritha, M.K.; Ramesh, R.; Hegde, R.; Kumar, S. Tactile Internet: Next Generation IoT. In Proceedings of the 2019 Third International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 10–11 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 22–26.
124. Promwongsa, N.; Ebrahimzadeh, A.; Naboulsi, D.; Kianpisheh, S.; Belqasmi, F.; Glitho, R.; Crespi, N.; Alfandi, O. A Comprehensive Survey of the Tactile Internet: State-of-the-Art and Research Directions. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 472–523. https://doi.org/10.1109/COMST.2020.3025995.
125. Eneyew, D.D.; Capretz, M.A.M.; Bitsuamlak, G.T. Toward Smart-Building Digital Twins: BIM and IoT Data Integration. *IEEE Access* **2022**, *10*, 130487–130506. https://doi.org/10.1109/ACCESS.2022.3229370.
126. Coupry, C.; Noblecourt, S.; Richard, P.; Baudry, D.; Bigaud, D. BIM-Based Digital Twin and XR Devices to Improve Maintenance Procedures in Smart Buildings: A Literature Review. *Appl. Sci.* **2021**, *11*, 6810. https://doi.org/10.3390/app11156810.
127. Hadjidemetriou, L.; Stylianidis, N.; Englezos, D.; Papadopoulos, P.; Eliades, D.; Timotheou, S.; Polycarpou, M.M.; Panayiotou, C. A Digital Twin Architecture for Real-Time and Offline High Granularity Analysis in Smart Buildings. *Sustain. Cities Soc.* **2023**, *98*, 104795. https://doi.org/10.1016/j.scs.2023.104795.
128. Chiariotti, F.; Condoluci, M.; Mahmoodi, T.; Zanella, A. SymbioCity: Smart Cities for Smarter Networks. *Trans. Emerg. Telecommun. Technol.* **2018**, *29*, e3206. https://doi.org/10.1002/ett.3206.
129. Sarathchandra, C.; Robitzsch, S.; Ghassemian, M.; Olvera-Hernandez, U. Enabling Bi-Directional Haptic Control in Next Generation Communication Systems: Research, Standards, and Vision. In Proceedings of the 2021 IEEE Conference on Standards for Communications and Networking (CSCN), Thessaloniki, Greece, 15–17 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 99–104.
130. Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. Tactile Internet and Its Applications in 5G Era: A Comprehensive Review. *Int. J. Commun. Syst.* **2019**, *32*, e3981. https://doi.org/10.1002/dac.3981.
131. Mekikis, P.-V.; Ramantas, K.; Antonopoulos, A.; Kartsakli, E.; Sanabria-Russo, L.; Serra, J.; Pubill, D.; Verikoukis, C. NFV-Enabled Experimental Platform for 5G Tactile Internet Support in Industrial Environments. *IEEE Trans. Ind. Inform.* **2020**, *16*, 1895–1903. https://doi.org/10.1109/TII.2019.2917914.
132. Baghalzadeh Shishehgarkhaneh, M.; Keivani, A.; Moehler, R.C.; Jelodari, N.; Roshdi Laleh, S. Internet of Things (IoT), Building Information Modeling (BIM), and Digital Twin (DT) in Construction Industry: A Review, Bibliometric, and Network Analysis. *Buildings* **2022**, *12*, 1503. https://doi.org/10.3390/buildings12101503.
133. Khajavi, S.H.; Motlagh, N.H.; Jaribion, A.; Werner, L.C.; Holmstrom, J. Digital Twin: Vision, Benefits, Boundaries, and Creation for Buildings. *IEEE Access* **2019**, *7*, 147406–147419. https://doi.org/10.1109/ACCESS.2019.2946515.
134. Arsenijević, D.; Stankovski, S.; Ostojić, G.; Baranovski, I.; Oros, D. An Overview of IoT Readiness Assessment Methods. In Proceedings of the 8th International Conference on Information Society and Technology, Kopaonik, Serbia, 11–14 March 2018; pp. 48–53.
135. Metwally, E.A.; Farid, A.A.; Ismail, M.R. Development of an IoT Assessment Method: An Interdisciplinary Framework for Energy Efficient Buildings. *Energy Build.* **2022**, *254*, 111545. https://doi.org/10.1016/j.enbuild.2021.111545.
136. *EN 15232*; European Committee for Standarization Energy Performance of Buildings—Impact of Building Automation, Controls and Building Management. European Commission: Brussels, Belgium, 2017.
137. *ISO 52120-1:2021*; I. 205 T.C. Energy Performance of Buildings Contribution of Building Automation, Controls and Building Management. International Organization for Standardization: Geneva, Switzerland, 2021.
138. Wei Wang; Lee, K.; Murray, D. Building a Generic Architecture for the Internet of Things. In Proceedings of the 2013 IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Melbourne, VIC, Australia, 2–5 April 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 333–338.
139. Wang, W.; Lee, K.; Murray, D. A Global Generic Architecture for the Future Internet of Things. *Serv. Oriented Comput. Appl.* **2017**, *11*, 329–344. https://doi.org/10.1007/s11761-017-0213-1.
140. Ali, Z.; Mahmood, A.; Khatoon, S.; Alhakami, W.; Ullah, S.S.; Iqbal, J.; Hussain, S. A Generic Internet of Things (IoT) Middleware for Smart City Applications. *Sustainability* **2022**, *15*, 743. https://doi.org/10.3390/su15010743.