Review

Not peer-reviewed version

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

Andrzej Ożadowicz *

Posted Date: 26 December 2023

doi: 10.20944/preprints202312.1994.v1

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

Review

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

Andrzej Ożadowicz

AGH University of Krakow, Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering, Department of Power Electronics and Energy Control Systems, 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 solution that support maintaining comfort, safety and improving energy efficiency in buildings. However, dynamically developing distributed network technologies, in particular the Internet of Things, 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 mix technologies of field-level and 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, along with a systematic review of the literature, case-studies and 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 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.

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 is 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 attempts are made by many research and engineering teams. This paper focuses on the applications of smart home as well as smart building systems and technologies, considering their inclusion in larger system structures like 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 ICT networks have been developing independently of each

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1994.v1

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, 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 twisted pair, less often power line, optical fiber or radio channels. Three open, international standards 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 on 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.

This trend has 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 filed 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 [3,5,13,19,23,27,28]:

- 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 reducing for wireless modules – sensors as well as 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 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 to develop many control and monitoring devices (network nodes) that are powerful to support control and data communication functions directly at the field-level, near the building infrastructure (for example temperature and occupancy sensors, various actuators – valves, motors etc.) [3,5,29]. In previous and some of existing solutions, most of the functions of control modules, along with 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) [30–33].

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 and effectively handle local workloads and make faster, more precise service decisions. Therefore, in smart home and smart building concept, one of the solutions turned out to be the expansion of the 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 and Artificial Intelligence – AI tools, 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 as well as consequently, various IoT and cloud services can be deployed on local systems. This paradigm is known as "edge computing" and it integrates IoT technologies and cloud computing systems [34,35]. What is very important in smart home and building applications, it reduces the communications' bandwidth needed between sensors, actuators as well as 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 [3,28,36]. 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 IoT edge modules in the 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 [34,35]. In [5] Taghizad-Tavana et al. explain that fog computing aims to optimize data transfer and communication between smart building zones, 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 [37,38] the fog computing paradigm is an alternative to smart modules with restricted 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, 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.) [34]. Finally, Nasir et al. [28] 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. Moreover, 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. These approach and its features are very important considering perspective of development 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 [5,6,39,40].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1994.v1

1.3. Original Contributions and the Paper Strucure

According to the information presented in the previous subsections, IoT technologies have a very wide application scope. This review focuses on the specific smart home and building systems industries, considering functionally of advanced BACS and BMS. Moreover, several technical aspects of interactive energy management with DSM and DSR functions for smart home and buildings operation within local microgrids and smart city infrastructures are discussed. 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:

- Providing a comprehensive review of the state-of-the art on IoT technics 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;
- Opposed to other IoT technology reviews, this one analyzes and discuss 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 new perspective on various IoT applications (e.g., edge and fog computing, big data processing) supported by recent research studies. To this end, this 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 as well as better integration;
- Presenting the major challenges, trends and pinpointing to new open research issues that need attention from researchers and domain experts, engineers. In particular, this review provides insight into the future scope of research on the integration of AI and ML capabilities, tactile internet developments, and IoT technology maturity assessment in building applications;
- Proposing general assumptions for generic IoT framework concept with SWOT analysis as well as pros and cons discussion.

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 buildings 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 framework for generic IoT 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 [41,42]. It should be noted that distributed solutions are the result of technological progress, development and miniaturization of electronics and they represent a significant achievement of 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, air-conditioning systems in houses, small buildings), where they work well and are attractively priced. However, distributed systems are becoming more and more popular in this sector as well. They are usually based on simple 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 [2,23,26,43,44]. 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 cloud, 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 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, equipped with microcontrollers and communication interfaces, necessary to exchange data (network variables and data points) between such modules. In the next stage of development process, with the increase in computing power and operating speed of microcontrollers (in the 2000s), universal programmable input/output modules appeared. Then automation servers and other system modules supporting the processing of growing amounts of data at the object level have been introduced [45–47]. As a result, especially in larger commercial and public buildings (e.g. hotels, shopping centers, office and university campuses), it became possible to build extensive automation and building management systems (BACS and BMS) with 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 communication protocols. In [44,47,48] the authors describe and explain their most important elements, pointing to the progressive hierarchization of the BACS network architecture. According to main assumptions the overall architecture for a typical BACS can be organized into three layers/levels depending upon functional hierarchy of specific application:

- *Field Layer*, the lowest one, where the interaction with field devices (sensors, actuators) happens as well as environmental data are collected, and parameters of the environment are physically controlled in response to commands from the system;
- *Automation Layer*, the middle layer, where data are processed, control loops are executed, and alarms are activated as well as processing entities also communicate values of more global interest to each other and values for vertical access by next management level are prepared (possibly aggregated);
- *Management Layer*, the top layer, where information from throughout the entire system is accessible as well as activities like system data presentation, forwarding, trending, logging, and archival 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 with 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, to be replaced by the expansion of TCP/IP, or should them exist together in a kind of symbiosis [20,49]?

In response, a broad, multi-aspect 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, taking up 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 [50–52]. Therefore, already in the first years of this process, research, engineering and methodological works were undertaken 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. [53] 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 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, 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 and actuators, etc. What is very important, the reaction of smart objects to events was pointed out, which is a key element of smart home and building systems, defined as event-based systems. In turn, in [54,55] papers 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 implementation of remote access, data acquisition and visualization in external services and 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 TCP/IP protocol is considered as crucial element of a standardization process of building automation protocols.

However, the second decade of the 2000s brings more and more analyzes 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 [56] 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 form 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, 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 use case study.

Going one step further, Lilis et al. [57] proposed a transitional design for BACS networks integrating IoT technologies. Based on the BACS architecture with field-level modules with communication in open standards (BACnet, KNX, LonWorks) and 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 the 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 [58,59].

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 – *Automation layer*.

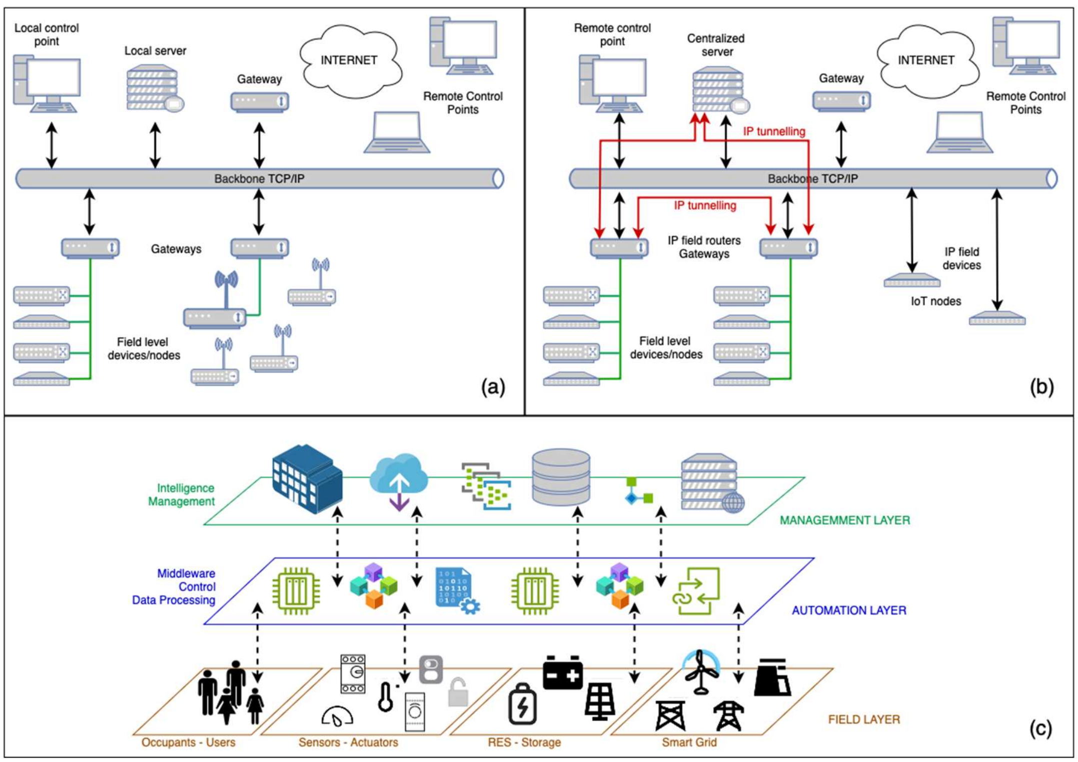

Figure 1. Schematic diagrams for two basic concepts of IoT development and application within the BACS and BMS architectures: (**a**) field-level devices connected by universal gateways to the higher network level using TCP/IP protocol and providing remote access [55]; (**b**) field-level devices connected by dedicated modules (automation servers, IP gateways) providing both remote access and data tunnelling (IP channel integrated within the BACS and BMS architecture) [45,56]; (**c**) additional distributed embedded electronics modules implemented at the automation level [57,58].

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 have 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 of implementing advanced control, monitoring and management functions of an increasing number of building infrastructure elements. 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 Oriented IoT and Edge and Fog Computing in BACS and BMS

Such a significant development of functional concepts indicating new development trends in BACS systems in smart home and building applications. Simultaneously the continuous development of IoT techniques and microcontrollers, determine 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 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 [35]. *Edge computing* can be defined as a computing approach that is using resources at 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 data are acquired by sensors and then send as control signals for actuators within the BACS [29,60,61]. The ongoing development of this layer of the BACS network, in particular the exchange of data in 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 [34,35]. *Fog computing* therefore operates at the *Automation* and *Management levels*, which are still supported the local network as well as external resources. Hence the fog element in the name, indicating a kind of blurring of the integrated network layers [37,38,40,60]. 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.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1994.v1

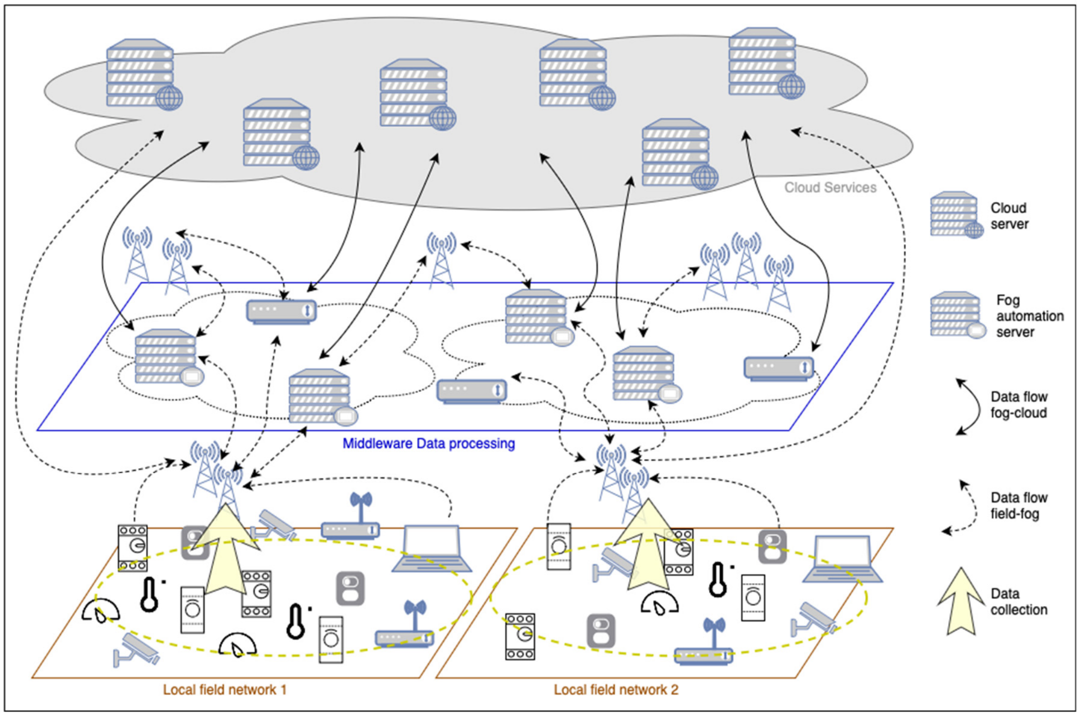

Figure 2. Structure and data flows in the network with field-level local networks, fog level as well as cloud level [40].

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 environment for a service oriented IoT [36] and a new Building as a Service (BaaS) [62] strategy. The first one is more general in nature, in the literature referred also as Fog of Everything (FoE) and Internet of Everything (IoE) and focuses on the abilities of using IoT technology in the implementation of services for four main areas: Processes, Data, People, 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.) [63].

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 [64,65] buildings, in particular non-residential, equipped with BACS and IoT distributed networks integrated with fog and cloud computing, can be perceived in the BaaS convention, defined as demand-oriented deployment of resources respectively assets. 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, 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. [64] 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) [66] and the related technical report [67] 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 analyzes 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 [33,68–70].

3.2. Big Data Processing and Cloud Computing

An aforementioned approach to BACS with IoT as a framework of 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 [71,72]. 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, multi-level structures of system networks are considered and developed. The key element of these analyzes 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. [73] propose an original cloud-fog computing architecture for information-centric IoT applications providing 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 [74] 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, sensitivity) in a very demanding time regime.

Research and development work are also carried out from a second perspective focused on the lowest levels of the network structure. In the 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 Microsoft Azure IoT Platform. Research focused on the functional capabilities of this solution and measurements of the system's effectiveness was carried out with results discussion. In other studies, Huang et al. [36] propose an edge intelligence framework for building 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 local system network. Further development of the concept is proposed by Nasir et al. [28] employing edge devices as a computational platform in terms of reducing energy costs and providing security, as well as remote control all field devices and appliances behind a

 doi:10.20944/preprints202312.1994.v1

secure gateway. Moreover, at the *Automation layer*, in addition to edge modules (nodes), they define fog nodes based on the powerful device Jetson Nano [75]. The platform is open for integration with external cloud services but considered only as an additional tool to perform the most advanced processing, data analysis and machine learning services.

In turn, in the paper [29] 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: a small apartment, a house, a small residential building, an office building, and a complex of smart buildings.

Finally, research and engineering works of the last few years are focused on the development of various, comprehensive concepts for organizing smart home and building systems with the IoT-edge-fog-cloud architecture. For instance, in [3,40,76] 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 providing services such as data aggregation and analytics, security, access control or self-healing, self-managing. The general diagram of such a network layer structure is shown in Figure 3.

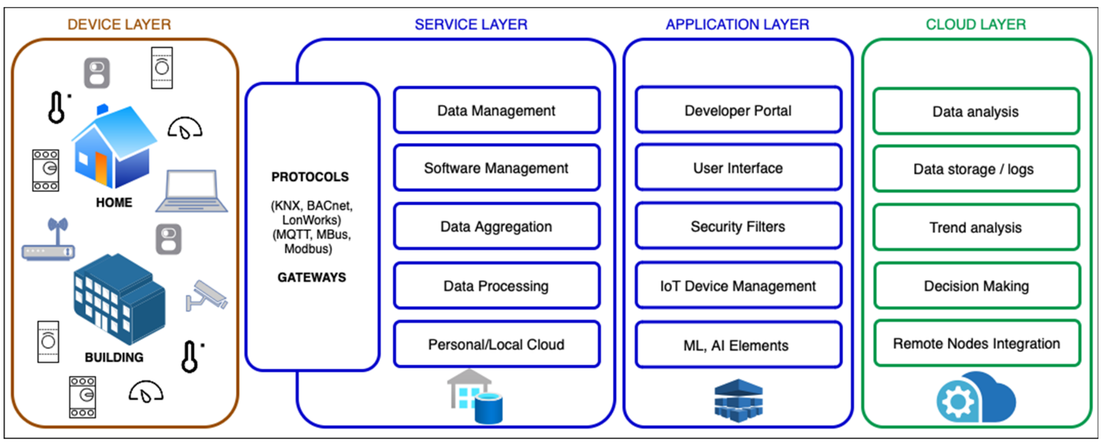

Figure 3. Advanced layer structure of BACS, BMS with IoT network, including big data processoing and cloud services [3,40,76].

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, ESP) or a class of microcomputers (e.g. Raspberry Pi, BeagleBone) 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 [60]. Additionally, a broader analysis of security issues and data transmission reliability in BACS and IoT *edge computing* networks in smart city applications was carried out 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 [77] traditional, conventional security mechanisms will not design or develop to secure such technology as IoT. Therefore, it is necessary to develop and introduce innovative solutions in the field of data security and reliable, trusted communication in such organized structures of smart home and building network. These issues are the subject of numerous research and technical analyses.

One of the most generalized analyzes is presented in [78], where the authors indicate the most important issues related to the security and privacy in 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/disposability (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 [78]:

- Heterogeneity of devices and communication, resulting from the coexistence of various modules/nodes in one network structure (from small sensors, relays, to large modules of automation servers, 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 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 number of humans on the globe and management of so large number of smart devices is very demanding task as well as inevitably raise the security risks;
- Privacy, IoT devices by their nature operate in a distributed structure, allowing communication in various wired and wireless technologies. This approach allows interaction everywhere, data communication with many other BACS network nodes, edge modules, in order to provide various services with different scope and resource use. The openness and flexibility of this structure generates additional privacy risks.

This is, of course, a very general summary. More threads emerge in detailed analyses. Particularly noteworthy is the paper [79], where Parikh et al. consider security and privacy risks for all three most important levels of IoT networks - cloud computing, fog computing and edge computing. The result of the analyzes is a classification of the complexity of problems and preliminary proposals for solutions, but without any technical or technological indications. In turn, the paper [34] 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 proposed models, mechanisms, and tools. Moreover, they discuss future research directions in this area considering balance between openness and ease of use the IoT networks as well as need of high level of their security and reliability.

From the point of view of BACS and BMS systems with IoT, the most important are countermeasures dedicated to fog and edge computing, integrated at the *Automation layer*, usually

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1994.v1

within a local subnet. Such countermeasures are described with detailed literature review by Alwakeel A. in [80], 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) [81] as well as port scanning attacks;
  d. Authentication schemes, where 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 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 [82];
  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 [83].

One of the most frequently discussed and analyzed solutions that are intended to support the implementation of most advanced security and privacy elements is blockchain ledger technology [34,80]. In relation to the IoT paradigm it is explained in [84] that blockchains, by definition, rely on a public directory acting as a common transaction information database for devices (nodes), edge modules as well as automation servers. Additionally, in [85] Moniruzzaman et al. discuss the blockchain-based smart home ecosystem with framework presented in Figure 4. According to them it is a four-layer conceptual framework consisting of four layers: (i) IoT data sources layer, (ii) blockchain network layer, (iii) smart home applications layer, and (iv) clients layer.

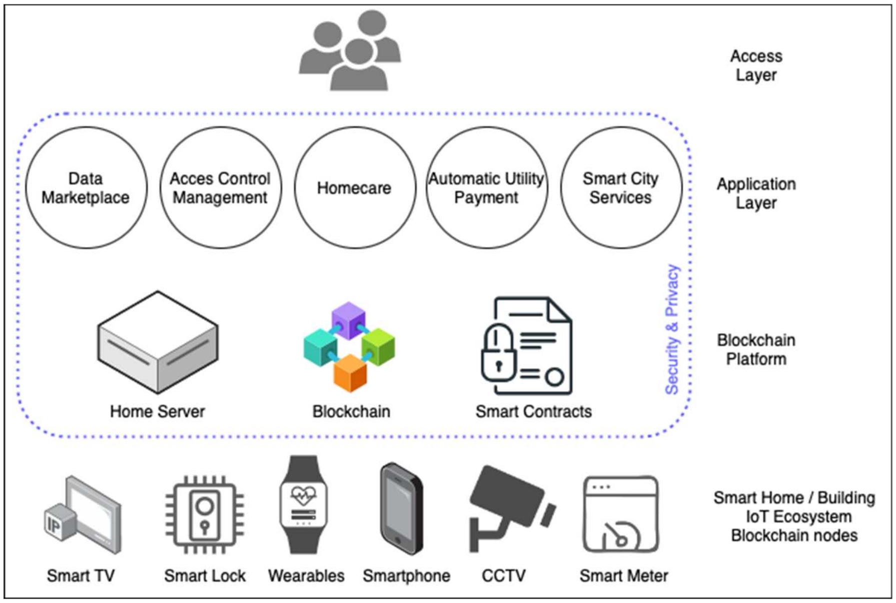

Figure 4. A four-layer application framework of a blockchain-based smart home ecosystem proposed and discussed in [85].

Sensors and actuators located in the first one generates and/or use data consolidated and stored in edge modules (servers) or a decentralized platform such as the second one – blockchain. All of the events and acts of the sensors and actuators became smart transactions, used to realize services. What is characteristic, time is an indestructible database that is placed in a new transaction and divided into a block hash chain. This way many copies of blocks are made and saved in the extracted nodes protocol. Moreover, hash values cryptographically connect blocks and edge modules (servers) may be considered as miners which are responsible for verifying and adding new transactions to new blocks while smart contracts follow predefined rules and facilitates the decentralized transactions [84,85]. 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 [86]. Additionally, it opens the way to easier and reliable integration with external services for instance in community microgrid frameworks suggested in [87].

Importantly, the more distributed network nodes in such a structure, the greater 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. Pros and cons related to the implementation of blockchain technology in IoT networks in various application areas, including smart home and buildings are discussed in [88,89], 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 [90]. 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 classic approach: scalability, storage and bandwidth, transaction charges (checking by miners), data privacy (sharing every node), network size (all nodes within network). In [77] 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 central authority unit, micro-transactions in real-time with zero fees, new scalable distributed ledger mechanism as well as 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 Artifical Inteligence

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. [91] in the context of BACS and BMS, the ML techniques could be used to solve fundamental problems such as predicting occupants' behavior and preferences, forecasting energy demand, peak periods which are difficult to be solved with traditional programming, but potential solutions can be achieved from advanced and fast data analyses. They reviewed several research and studies and discuss 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 *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 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 [12,92];
   b. Appliance profiling and fault detection to track and identify different building's appliances as well as detect anomalies/failures in the different components of the energy management system. Moreover, this approach allows to support DSM and DSR mechanisms of transactive energy [93,94].

These two categories are mostly discussed in the context of ML applications within smart home and buildings. In [95] the authors analyze in detail various technical and functional aspects of human activity recognition in smart homes using algorithms for IoT sensor networks, considering pros and cons of different ML methods and tools dedicated for various smart home and building applications. However, in [96] Suman et al. point out that in turn advanced IoT and BACS devices may impact the behavior of people in buildings. Based on human as well as 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 [97] 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 saving. 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 [98] the authors identify most essential BACS with IoT enabled factors that sanction a need of ML as well as AI integration with smart homes and buildings to provide energy efficiency improvements and facilitate energy management. Research, analyzes and case studies are carried out in this area, using advanced functionalities and communication techniques [30,69,99–101].

Another issue is the possibility of using ML mechanisms with AI elements to recognize, classify and service BACS and IoT modules, network nodes. Cvitic et al. [102] propose original approach and ML based IoT device classification model considering various sets of data and different data traffic models. Moreover, considering growing of the BACS with IoT solutions, especially with edge and fog computing, Huang et al. [36] note that real-time detection of unexpected, emergent or spontaneous situations is important to increase the reliability of the network and improve 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 undertaken aimed at developing 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 [103–105]. 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 [106–108].

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

 doi:10.20944/preprints202312.1994.v1

important since in classic BACS and IoT networks design and architecture development each control function, rule only works in one subsystem (e.g. HVAC, lighting, security etc.) and there is no interoperability between these subsystems (or it is very limited). 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 [109] Panchalingam et al. describe several smart building domains that should be considered for integration with AI techniques with 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 [110] and [111] considering not only functional and organizational aspects, but technical architectural as well.

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

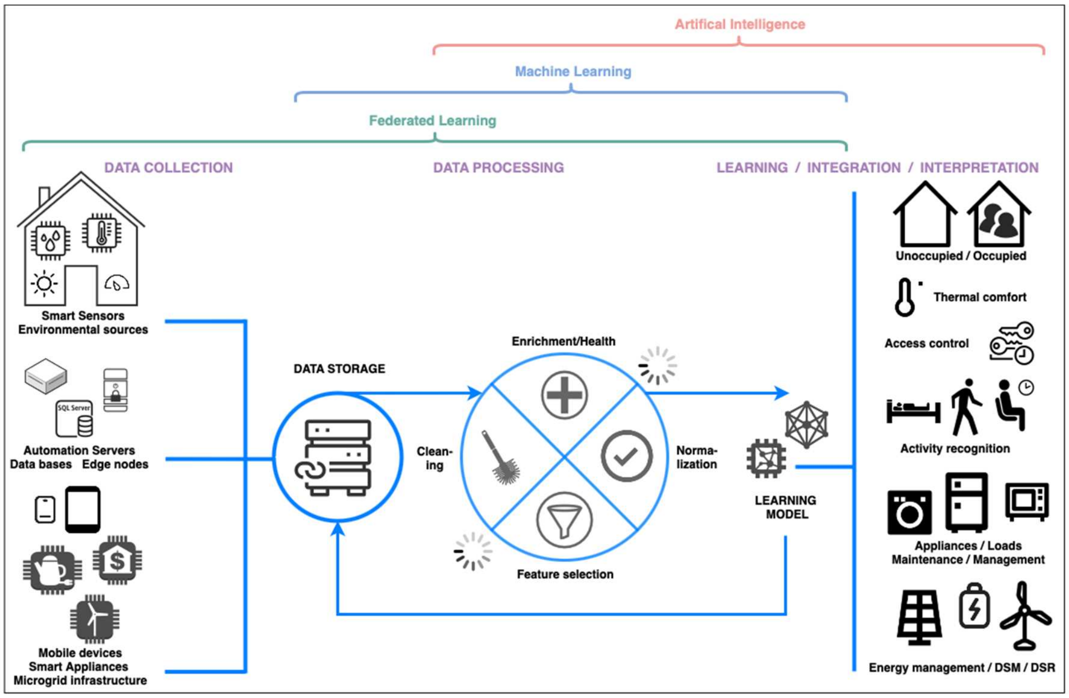

Figure 5. The BACS with IoT systems areas for implementation of ML, FL and AI techniques, methods and tools (based on [91]).

4.2. Tactile Internet, Digital Twins with Distributed Automation Newtowrks

All these methods and technologies - ML, FL and AI, become the basis for the implementation of new functional possibilities and development of emerging trends of BACS, BMS systems with IoT. The author has selected two, 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, as well as operational maintenance support techniques, especially for large BMS with IoT systems in smart buildings.

The first one is Tactile Internet or Tactile Internet of Things (TIoT) considered as the second generation of 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 [103,112]. In its most basic approach, TIoT involves wireless communication (5G, WiFi) and classic wired channels to control of real and virtual objects (actuators) by humans in real time. 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, industry [113,114]. 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. [113] point out, crucial design goals can be achieved by placing TIoT nodes close to each other, which is possible with distributed, 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 [113,115]. However, the implementation of user interfaces and functions in the haptic, 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 [103,112–114].

The second selected 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 [116,117] the BIM is used in architecture, construction, engineering and facility management to facilitate the planning, 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 [116] the authors point out the two most important differences between DT and BIM: (i) the BIM was designed to improve the efficiency of design and construction and still it is used in these processes, but the DT is designed to monitor a physical assets and improve their operational efficiency as well as to provide predictive maintenance; (ii) the BIM was not designed to work with real-time data therefore it is used for design, construction facility management, whereas the DT is a dynamic environment, with support for real-time data and ML and AI. Moreover, in [118] 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 electricity meters installed in the building to monitor its real-time operating conditions. Additionally, live weather data could be collected as well. These live data are directly incorporated as inputs into simulation tools to replicate the building operating conditions in real time;
3. Simulation tools with model-based modeling are incorporated to simulate the 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 to integrate monitoring and control applications and to investigate different what-if scenarios.

This architecture is presented in the graphical form in Figure 6, published and described in detail in the paper [119]. Moreover, the dependencies between BIM and DT techniques in terms of their use in distributed systems with IoT are analyzed in the paper [120].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1994.v1

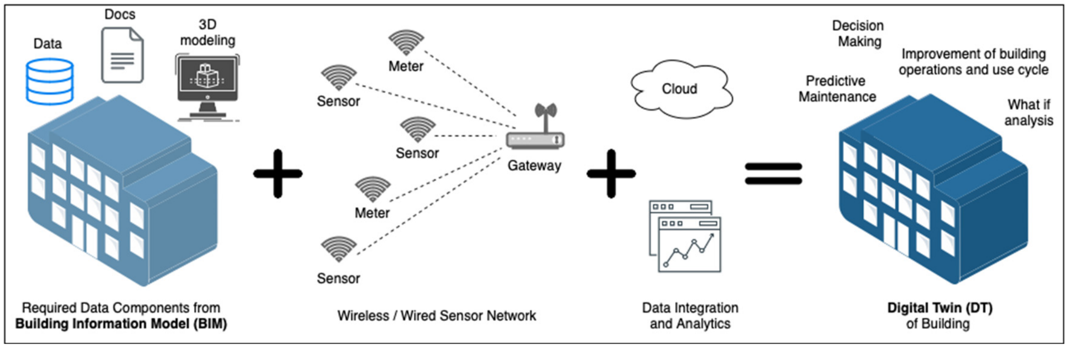

Figure 6. Essential components of building DT architecture [119].

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 to conduct active energy management mechanisms, demand and load prediction as well as provide control and monitoring functions [116,117].

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 raises 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 the last few years, attempts have been made to develop IoT readiness assessment methods and tools. They focus in particular on the evaluation of two areas: the technical and organizational condition 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 [121] Arsenijevic et al. describe four possible methods for assessing IoT technological maturity with varying levels of detail. The most important verification factors were analyzed, in particular related to the network structure (centralized, distributed), available computing power and data analytics tools, diversity of standards and data transmission protocols in the system, but also the readiness of the IT team to support new networks with edge and fog elements. and cloud computing. In turn, in the paper [122] Metwally et all. analyze these methods in detail, along with additional technical and organizational aspects relating directly to IoT applications in BACS, BMS. As result they proposed their own scale and indicator for assessing IoT readiness with five levels of advancement:

Low IoT Level, larger manual, low automatic control at the building level (local automation);

1. 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;
2. High IoT Level, automatic control at the building level (distributed automation), with networked sensors and modules-nodes to control most systems' functions with the performance analysis;
3. Fully IoT Level, automatic control across all buildings/site levels (distributed networked automation) with networked sensors, all modules-nodes to control most systems' functions with the performance analysis also perform a predictive decision making.

A similar approach is presented by the authors of the paper [1] where, after a comprehensive analysis of existing methods of verifying technological maturity and readiness for IoT solutions, they also proposed a four-level IoT assessment model, but with an additional level zero. This model, however, relates mainly to organizational issues of preparation of staff and teams operating 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 [123,124] and the assessment of the readiness of buildings for intelligent solutions and smart grid networks with the Smart Readiness Indicator (SRI) – EPBD directive [66] and technical report [67].

5. Generic IoT Framework – Concept, Development and Discussion

Bearing in mind all technical and organizational aspects analyzed in sections 2-4 of this review, the author proposes systematizing the most important elements relating to technical, organizational and conceptual issues, in the perspective of developing the concept and implementing the so-called generic IoT [125–127]. 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.

In the next subsections there is a structured framework proposed, outlining both mandatory and optional elements as well as considering specific requirements for smart home and building applications, including edge, fog, and cloud computing.

5.1. Manadatory 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 whole system with BACS and IoT nodes. They are divided in six levels.

Device Layer: Sensors and actuators form the foundation of the field-level within the network, enabling data collection and control, essential for smart decision-making both in building automation and smart homes.

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 3.

Data Processing Layer: *Edge computing* enhances real-time data processing near the device level within local network, reducing latency and ensuring timely responses, while data filtering and aggregation optimize network resources.

Integration Layer: BIM and DT based on TCP/IP protocol as well as middleware enable the harmonious integration of IoT devices with building structures and diverse systems, promoting a cohesive and interoperable environment.

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, BMS IoT ecosystem.

Cloud Computing Layer: Leveraging cloud storage and ensuring scalability supports the archiving of historical data, large-scale analytics, and accommodates the evolving nature of generic IoT systems.

It should be noted that these mandatory elements collectively establish a solid foundation for a reliable, secure, and integrated generic IoT framework. They address 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 IoT technologies integrated.

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 smart home and smart building.

5.2.1. Smart Home Applications

Remote Access and Control: mobile applications development to provide homeowners and users with remote access for monitoring and controlling smart home devices; implementation and integration of voice commands for hands-free and convenient control.

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.

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.

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.

ML and AI: utilizing ML for predictive analytics in smart building management, optimizing resource allocation and improving overall efficiency; implementing of AI-based anomaly detection for proactive identification of faults and irregularities in building automation systems.

Regulatory Compliance: ensure robust data privacy measures to comply with regulations, addressing the unique challenges associated with handling sensitive data in smart building applications; compliance with energy efficiency standards where specific energy efficiency standards applicable to commercial and large-scale buildings must be complied with.

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 smart home and BACS, 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;

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 December 2023 doi:10.20944/preprints202312.1994.v1

- 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 as well as 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 framework's credibility 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 it requires consideration when implemented in smart home applications. The underlying integration of BACS and BMS techniques with IoT poses challenges including the potential complexity of implementation, intensity of use of resources available in 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.

6. Conclusions

IoT technologies set the directions 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 this type 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 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 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.

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

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
BaaS	Building as a Service
BACS	Building Automation and Control Systems
BIM	Building Information Modeling
BMS	Building Management Systems
DoS	Denial-of-Service
DSM	Demand Side Management
DSR	Demand Side Response
DT	Digital Twin
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
IoE	Internet of Everything
IoT	Internet of Things
IOTA	Internet of Things Application
ML	Machine Learning
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
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, doi: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. *Applied Sciences* **2023**, *13*, 7745, doi: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, doi: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, doi: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, doi:10.3390/su142315938.

6. Sharma, H.; Haque, A.; Blaabjerg, F. Machine Learning in Wireless Sensor Networks for Smart Cities: A Survey. *Electronics (Basel)* **2021**, *10*, 1012, doi: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, doi:10.1109/ACCESS.2020.2979022.
8. International Organization for Standardization ISO/IEC 14543-3-10:2020 Information Technology Home Electronic Systems (HES) Architecture - KNX; Geneva, Switzerland , 2020;
9. International Organization for Standardization ISO/IEC 14908-1:2012 Information Technology Control Network Protocol - LonWorks; Geneva, Switzerland , 2012;
10. International Organization for Standardization *ISO 16484-6:2020 Building Automation and Control Systems (BACS) - BACnet*; Geneva, Switzerland , 2020;
11. Bovet, G.; Hennebert, J. Will Web Technologies Impact on Building Automation Systems Architecture? *Procedia Comput Sci* **2014**, *32*, 985–990, doi: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 (Basel)* **2017**, *10*, 1771, doi: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. *Journal of Sensor and Actuator Networks* **2022**, *11*, 74, doi: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, doi: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); IEEE, October 6 2022; pp. 229–234.
16. Secgin, S. Seven Layers of ISO/OSI. In *Evolution of Wireless Communication Ecosystems*; Wiley, 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, 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); IEEE, October 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, doi: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); IEEE, June 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); IEEE, June 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, doi: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, doi:10.3390/fi15090316.
24. Prakosa, S.; Nugraha, A.; Atiq, M.' Miniature SmartHome Dengan Sonoff. *Jurnal Riset Rumpun Ilmu Teknik (JURRITEK)* **2023**, *2*.
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, doi: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; Institute of Electrical and Electronics Engineers Inc., 2023.
27. Singhai, R.; Sushil, R. An Investigation of Various Security and Privacy Issues in Internet of Things. *Mater Today Proc* **2023**, *80*, 3393–3397, doi:10.1016/j.matpr.2021.07.259.
28. 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, doi:10.1016/j.neucom.2021.04.138.
29. 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, doi:10.3390/s22031002.
30. Babar, M.; Grela, J.; Ożadowicz, A.; Nguyen, P.; Hanzelka, Z.; Kamphuis, I. Energy Flexometer: Transactive Energy-Based Internet of Things Technology. *Energies (Basel)* **2018**, *11*, 568, doi:10.3390/en11030568.

31. Faqiry, M.; Edmonds, L.; Zhang, H.; Khodaei, A.; Wu, H. Transactive-Market-Based Operation of Distributed Electrical Energy Storage with Grid Constraints. *Energies (Basel)* **2017**, *10*, 1891, doi:10.3390/en10111891.
32. 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 Electrification Magazine* **2016**, *4*, 8–14, doi:10.1109/MELE.2016.2614188.
33. Ożadowicz, A. A Hybrid Approach in Design of Building Energy Management System with Smart Readiness Indicator and Building as a Service Concept. *Energies (Basel)* **2022**, *15*, 1432, doi:10.3390/en15041432.
34. 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, doi:10.1016/j.comcom.2021.09.003.
35. 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. *Journal of Systems Architecture* **2019**, *98*, 289–330, doi:10.1016/j.sysarc.2019.02.009.
36. 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 Generation Computer Systems* **2018**, *87*, 557–567, doi:10.1016/j.future.2018.03.003.
37. 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 Generation Computer Systems* **2020**, *103*, 18–27, doi:10.1016/j.future.2019.09.045.
38. 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 Beniamino and Li, K.-C. and Y.L.T. and E.A., Ed.; Springer Singapore: Singapore, 2018; pp. 103–130.
39. Alnajar, O.; Barnawi, A. Tactile Internet of Federated Things: Toward Fine-Grained Design of FL-Based Architecture to Meet TIoT Demands. *Computer Networks* **2023**, *231*, 109712, doi:10.1016/j.comnet.2023.109712.
40. 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, doi:10.1007/s12083-019-00783-7.
41. 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, doi:10.1016/j.apenergy.2021.118408.
42. Ge, X.; Yang, F.; Han, Q. Distributed Networked Control Systems: A Brief Overview. *Inf Sci (N Y)* **2017**, *380*, 117–131, doi:10.1016/j.ins.2015.07.047.
43. Islam, R.; Rahman, Md.W.; Rubaiat, R.; Hasan, Md.M.; Reza, Md.M.; Rahman, M.M. LoRa and Server-Based Home Automation Using the Internet of Things (IoT). *Journal of King Saud University - Computer and Information Sciences* **2022**, *34*, 3703–3712, doi:10.1016/j.jksuci.2020.12.020.
44. Bhatt, J.; Verma, H.K. Design and Development of Wired Building Automation Systems. *Energy Build* **2015**, *103*, 396–413, doi:10.1016/j.enbuild.2015.02.054.
45. Merz, H.; Hansemann, T.; Hübner, C. *Building Automation*; Signals and Communication Technology; Springer International Publishing: Cham, 2018; ISBN 978-3-319-73222-0.
46. Dietrich, D.; Bruckner, D.; Zucker, G.; Palensky, P. Communication and Computation in Buildings: A Short Introduction and Overview. *IEEE Transactions on Industrial Electronics* **2010**, *57*, 3577–3584, doi:10.1109/TIE.2010.2046570.
47. Wang, S. *Intelligent Buildings and Building Automation*; Routledge, 2009; ISBN 9781134025107.
48. Domingues, P.; Carreira, P.; Vieira, R.; Kastner, W. Building Automation Systems: Concepts and Technology Review. *Comput Stand Interfaces* **2016**, *45*, 1–12, doi:10.1016/j.csi.2015.11.005.
49. Lobaccaro, G.; Carlucci, S.; Löfström, E. A Review of Systems and Technologies for Smart Homes and Smart Grids. *Energies (Basel)* **2016**, *9*, 1–33, doi:10.3390/en9050348.
50. 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).
51. 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).
52. EXOR Powerful IoT-Ready Interfaces with KNX Interface Available online: https://www.exorint.com/corporate/press-release/knx-2020 (accessed on 8 December 2023).
53. 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, doi:10.1109/MIC.2009.143.

54. 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; IEEE, May 2011; pp. 423–427.
55. 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); IEEE, January 2011; pp. 292–296.
56. 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; IEEE, July 2012; pp. 683–688.
57. 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, doi:10.1016/j.scs.2016.08.019.
58. 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); IEEE, June 2015; pp. 1–8.
59. 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); IEEE, September 2017; pp. 1–6.
60. 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 (Basel)* **2023**, *16*, 3465, doi:10.3390/en16083465.
61. 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); IEEE, February 2018; pp. 452–457.
62. BaaS Consortium Partners Building as a Service. Final Report of the Project Funded by the European Community in the 7 Th Framework Programme ICT for Sustainable Growth; 2016;
63. 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, doi:10.1109/ACCESS.2017.2702013.
64. Wildenauer, A.; Mbabu, A.; Underwood, J.; Basl, J. Building-as-a-Service: Theoretical Foundations and Conceptual Framework. *Buildings* **2022**, *12*, 1594, doi:10.3390/buildings12101594.
65. Wildenauer, A.; Basl, J. Building-as-a-Service: The Opportunities of Service-Dominant Logic for Construction. *Marketing Science & Inspirations* **2022**, *17*, 41–53, doi:10.46286/msi.2022.17.3.5.
66. European Parliament Directive (EU) 2018/844 of the European Parliament and the Council on the Energy Performance of Buildings; EU, 2018;
67. Verbeke Stijin; Aerts Dorien; Reynders Glenn; Ma Yixiao; Waide Paul FINAL REPORT ON THE TECHNICAL SUPPORT TO THE DEVELOPMENT OF A SMART READINESS INDICATOR FOR BUILDINGS; 2020;
68. Ramezani, B.; Silva, Manuel.G. da; Simões, N. Application of Smart Readiness Indicator for Mediterranean Buildings in Retrofitting Actions. *Energy Build* **2021**, *249*, 111173, doi:10.1016/j.enbuild.2021.111173.
69. 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 (Basel)* **2019**, *12*, 2896, doi:10.3390/en12152896.
70. 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, doi:10.3390/su12229496.
71. 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); IEEE, September 8 2021; pp. 1–6.
72. 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); IEEE, June 7 2022; pp. 1–6.
73. 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); IEEE, May 2017; pp. 637–640.
74. 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, doi:10.1007/s12145-020-00481-6.
75. NVIDIA Developer Jetson Nano Developer Kit Available online: https://developer.nvidia.com/embedded/jetson-nano-developer-kit (accessed on 14 December 2023).

76. 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, doi:10.3390/s21144932.
77. 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, doi:10.1109/ACCESS.2021.3138353.
78. Singhai, R.; Sushil, R. An Investigation of Various Security and Privacy Issues in Internet of Things. *Mater Today Proc* **2023**, *80*, 3393–3397, doi:10.1016/j.matpr.2021.07.259.
79. 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, doi:10.1016/j.procs.2019.11.018.
80. Alwakeel, A.M. An Overview of Fog Computing and Edge Computing Security and Privacy Issues. *Sensors* **2021**, *21*, 8226, doi:10.3390/s21248226.
81. 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); IEEE, July 14 2021; pp. 763–768.
82. 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); IEEE, June 1 2022; pp. 122–130.
83. 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); IEEE, August 2018; pp. 1097–1106.
84. Alam, T. Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges. *Computers* **2022**, *12*, 6, doi:10.3390/computers12010006.
85. Moniruzzaman, Md.; Khezr, S.; Yassine, A.; Benlamri, R. Blockchain for Smart Homes: Review of Current Trends and Research Challenges. *Computers & Electrical Engineering* **2020**, *83*, 106585, doi:10.1016/j.compeleceng.2020.106585.
86. Taneja, S.; Rana, I.; Tyagi, S. Blockchain for Iot Security and Privacy: Smart Home-A Review. *International Journal of Advances in Engineering and Management (IJAEM)* **2023**, *5*, 1293, doi:10.35629/5252-050512931296.
87. 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, doi:10.1109/ACCESS.2020.2975233.
88. 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, doi:10.3390/s23020947.
89. 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, doi:10.1109/ACCESS.2020.3004662.
90. 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, doi:10.1007/s11277-023-10226-5.
91. Djenouri, D.; Laidi, R.; Djenouri, Y.; Balasingham, I. Machine Learning for Smart Building Applications. *ACM Comput Surv* **2020**, *52*, 1–36, doi:10.1145/3311950.
92. Shayeghi, H.; Shahryari, E.; Moradzadeh, M.; Siano, P. A Survey on Microgrid Energy Management Considering Flexible Energy Sources. *Energies (Basel)* **2019**, *12*, 2156, doi:10.3390/en12112156.
93. 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, doi:10.1016/j.eng.2022.03.001.
94. 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, doi:10.1109/TSG.2013.2268664.
95. 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, doi:10.3390/s21186037.
96. Suman, S.; Etemad, A.; Rivest, F. Potential Impacts of Smart Homes on Human Behavior: A Reinforcement Learning Approach. *IEEE Transactions on Artificial Intelligence* **2022**, *3*, 567–580, doi:10.1109/TAI.2021.3127483.
97. 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 (Basel)* **2020**, *13*, 1097, doi:10.3390/en13051097.
98. 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. *Applied Sciences* **2022**, *12*, 7882, doi:10.3390/app12157882.
99. Kawa, B.; Borkowski, P. Integration of Machine Learning Solutions in the Building Automation System. *Energies (Basel)* **2023**, *16*, 4504, doi:10.3390/en16114504.

100. 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. *Renewable and Sustainable Energy Reviews* **2022**, *164*, 112482, doi:10.1016/j.rser.2022.112482.
101. 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 (Basel)* **2020**, *13*, 5128, doi:10.3390/en13195128.
102. Cvitić, I.; Peraković, D.; Periša, M.; Gupta, B. Ensemble Machine Learning Approach for Classification of IoT Devices in Smart Home. *International Journal of Machine Learning and Cybernetics* **2021**, *12*, 3179–3202, doi:10.1007/s13042-020-01241-0.
103. Alnajar, O.; Barnawi, A. Tactile Internet of Federated Things: Toward Fine-Grained Design of FL-Based Architecture to Meet TIoT Demands. *Computer Networks* 2023, *231*.
104. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A Survey on Federated Learning. *Knowl Based Syst* **2021**, *216*, 106775, doi:10.1016/j.knosys.2021.106775.
105. Mammen, P.M. Federated Learning: Opportunities and Challenges. **2021**.
106. 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*.
107. 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, doi:10.1016/j.compind.2022.103801.
108. 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, doi:10.1109/MNET.011.2000514.
109. Panchalingam, R.; Chan, K.C. A State-of-the-Art Review on Artificial Intelligence for Smart Buildings. *Intelligent Buildings International* **2021**, *13*, 203–226, doi:10.1080/17508975.2019.1613219.
110. 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 of Things* **2023**, *22*, 100772, doi:10.1016/j.iot.2023.100772.
111. Genkin, M.; McArthur, J.J. B-SMART: A Reference Architecture for Artificially Intelligent Autonomic Smart Buildings. *Eng Appl Artif Intell* **2023**, *121*, 106063, doi:10.1016/j.engappai.2023.106063.
112. Hou, Z.; She, C.; Li, Y.; Niyato, D.; Dohler, M.; Vucetic, B. Intelligent Communications for Tactile Internet in 6G: Requirements, Technologies, and Challenges. *IEEE Communications Magazine* **2021**, *59*, 82–88, doi:10.1109/MCOM.006.2100227.
113. Fanibhare, V.; Sarkar, N.I.; Al-Anbuky, A. A Survey of the Tactile Internet: Design Issues and Challenges, Applications, and Future Directions. *Electronics (Basel)* **2021**, *10*, 2171, doi:10.3390/electronics10172171.
114. N., A.; Rai, K.H.J.; M.K., H.; 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); IEEE, January 2019; pp. 22–26.
115. 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 Communications Surveys & Tutorials* **2021**, *23*, 472–523, doi:10.1109/COMST.2020.3025995.
116. 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, doi:10.1109/ACCESS.2022.3229370.
117. 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. *Applied Sciences* **2021**, *11*, 6810, doi:10.3390/app11156810.
118. 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, doi:10.1016/j.scs.2023.104795.
119. 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, doi:10.1109/ACCESS.2019.2946515.
120. 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, doi:10.3390/buildings12101503.
121. 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; 2018; pp. 48–53.
122. Metwally, E.A.; Farid, Ayman.A.; Ismail, M.R. Development of an IoT Assessment Method: An Interdisciplinary Framework for Energy Efficient Buildings. *Energy Build* **2022**, *254*, 111545, doi:10.1016/j.enbuild.2021.111545.

 doi:10.20944/preprints202312.1994.v1

123. EN 15232; European Committee for Standarization Energy Performance of Buildings - Impact of Building Automation, Controls and Building Management; Brussels, 2017;
124. ISO 52120-1:2021, I. 205 T.C. Energy Performance of Buildings Contribution of Building Automation, Controls and Building Management; Geneva, Switzerland, 2021;
125. 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, doi:10.3390/su15010743.
126. 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; IEEE, April 2013; pp. 333–338.
127. Wang, W.; Lee, K.; Murray, D. A Global Generic Architecture for the Future Internet of Things. *Service Oriented Computing and Applications* **2017**, *11*, 329–344, doi:10.1007/s11761-017-0213-1.