NTU JOURNAL OF ENGINEERING AND TECHNOLOGY RESEARCH ARTICLE
E-ISSN:2788-998X Open Access

Communication and Network Technologies of IoT in Smart Building: A Survey

Salar Jamal Rashid[1,2], Ahmed Maamoon Alkababji[2], AbdulSattar Mohammed Khidhir[3]
{ salar.jamal@ntu.edu.iq[1], ahmedalkababji72@uomosul.edu.iq[2], abdulsattarmk@ntu.edu.iq[3]}

1.Computer Center, Northern Technical University, Mosul, Iraq, 2. Department of Computer Engineering, College of Engineering, Mosul University, Mosul, Iraq, 3. Department of Computer Systems, Mosul Technical Institute, Northern Technical University, Mosul, Iraq

Corresponding author: Salar Jamal Rashid, e-mail: { salar.jamal@ntu.edu.iq }
Co-authors: Ahmed M. Alkababji: ahmedalkababji72@uomosul.edu.iq,
AbdulSattar M. Khidhir: abdulsattarmk@ntu.edu.iq

Received: 13-09-2021, **Accepted:** 13-10-2021, **Published online:** 28-10-2021

Abstract: Many industries are incorporating the Internet of Things (IoT) into their daily operations. Examples include smart homes, smart grids, smart cities, logistics, e-health, and physical security. An IoT-enabled smart building provides support for IoT applications that offer both quality and cost-effectiveness. Smart buildings are important places to deal with and manage all kinds of operating conditions, such as lighting, ventilation, humidity, temperature, safety, and others. Furthermore, it is crucial to establish living spaces with better well-being standards and an enhanced quality of life. Additional problems that smart buildings create include the diversity of communication technologies and the inflexible architecture of the building. These issues include complications related to application and IoT device heterogeneity, efficient energy, security, and appropriate automation systems. This paper presents a survey of many researches on IoT in smart buildings, which have been categorized into five important smart building applications: energy, localization, comfort, automation, and security. The survey is based on the most used communication technologies in smart buildings; the connectivity standards (PLC, PoE, RFID, Bluetooth, BLE, WIFI, UWB), transmission protocols (IPv6, 6LoWPAN, ZigBee, Z-wave, CoAP and MQTT), network topologies (Bus, Star, Mesh, Tree) and network area (PAN, LAN, WAN).

Keywords: IoT, Smart Building, Communication Technologies, Applications.

1. Introduction

The exponential growth in the number of things connected to the Internet is resulting in the enrichment of the digital world [1]. In a wide range of domains, the Internet of Things (IoT) is improving and enhancing human life and work efficiency [2]. The use of IoT devices to make buildings smarter and more efficient is growing rapidly [3].

The IoT is a network of physical objects made up of sensors, software and electronics that are capable of communicating with each other and the users. This is rapidly evolving because of the convergence between communication technologies and the internet [4].

More IoT devices are being connected every day all over the world. According to Cisco, the total number of interconnected objects on the planet surpassed the total number of humans in 2011 [5]. also, Cisco reported that by 2020, there will be 50 billion connected objects, resulting in significant changes and developments in the digital domain. IoT is improving human life in a variety of ways and will continue to do so in the future [6].

One of the uses of IoT in the urban area is smart building applications, which promise to improve people' quality of life through the use of Information and Communications Technology (ICT) [4].

IoT sensors monitor the environment continuously inside buildings, and data from these sensors can be stored and managed on a server, where it can be collected, transformed, and examined in real-time or on demand [7].

Smart buildings need architecture that can handle vast amounts of information and perform computation, all of this based on communication standards and Internet protocols using advanced information processing paradigms [8].

Buildings, among other physical objects, are playing an essential part in this technological revolution. Buildings serve as human habitats, such as domestic structures, or for specific purposes, such as schools, shops, storehouses, or industrial structures. They can serve both purposes in some cases. There are several aspects of modern-day building operations that can be automated and optimized further [9]. It has been proven that improved energy management through automation has significant benefits; additionally, adaptation to preferences human-friendliness and building security can all be improved. Smart buildings and smart cities are now under much research, and they promise to dramatically improve our lives, while also increasing sustainability and the environment. Most building automation systems have traditionally been designed for specific applications and have limited openness and flexibility. The chance of changing this state of affairs is growing rapidly, thanks to the rapid maturation of several supporting technologies. [10].

There have been several survey researches published that cover various fields of IoT technologies. For example, Atzori et al. [11] conducted a survey that covered the main enabling communication technologies, both wireless and wired, as well as the components of wireless sensor networks (WSN). Al-Fuqaha et al. [12] conducted a survey that introduced the protocols, enabling technologies, and potential applications of IoT and the key challenges to point out future directions. The authors of [13] discussed IoT architecture as well as the challenges of developing and deploying IoT applications. Andrea et al. [14] conducted a survey that examined the security issues and challenges in IoT from the perspectives of physical systems, networks, applications, as well as the privacy and security issues in technologies related to physical systems, software, encryption, and networking. The authors of [15] provided an overview of the IoT for particular clinical wireless devices that use Bluetooth, 6LoWPAN, IEEE 802.15.4, and Near-Field Communication (NFC) for eHealth and mHealth applications. Furthermore, Yang et al. [16] discussed the IoT enabling technologies, with a focus on Radio Frequency Identification (RFID) and its possible applications. The authors in [17] presented IoT challenges in order to fill the gap between research and application. In [18] the authors provided an overview of current IETF challenges and standards for the IoT. Our survey will concentrate on the most used communication technologies including connectivity, network protocols, network topologies and areas in IoT under smart building environment. Many key applications will be studied including energy, localization, comfort, automation and security issues.

The paper is organized as follows: Section 2 provides a background theory of IoT and smart building and the relation between them. Section 3 presents the most key application used in smart building. Section 4 discuss the communicating and networking technologies used in IoT based smart building. Section 5 shows our survey of many researches regarding the key application with the communication technologies.

2. Background Theory

2.1 Internet of Thing (IoT)

The term IoT describes a system in which the digital and physical worlds are linked to form a worldwide network [19-20]. IoT exploits actuators, sensors, and data communication technologies embedded into physical objects (e.g., in the case of smart buildings: lifts, facades, windows, furniture, walls, water systems, roofs, lighting modules, heating/cooling modules, ventilation modules, equipment, electrical communication systems, power systems and storage systems etc.). This permits the tracking, coordination or control of such objects across data networks or internet to create value for the user throughout the life cycle of the system [21].

Within the next few years, IoT has spread quickly and will continue to spread. This emerging technology field will open up new perspectives and features of services, which will lead to an enhanced consumer quality of life and also demonstrate successful in productivity for businesses [22]. For consumers, IoT is able to offer solutions in different sectors, including healthcare, safety, energy efficiency, comfort and many more. IoT can improve productivity, storage management, product and item tracking, agriculture and decision-making at company level drastically. In the recent years a significant amount of research has been undertaken in the IoT field, aimed specifically at smart environments such as smart cities, smart grids, smart buildings, and so forth [23].

IoT is increasingly seen as a solution to the growing demand for interconnection between devices, people, gadgets, companies, and organizations, and it arose from a desire to gain real-time access and control over information so that integrated resources can be managed optimally and intelligently.

Based on the concept of Machine to Machine (M2M) connectivity, optimized by the advances of smart actuators and sensors, together with communication technologies (Bluetooth, WIFI, NFC, RFID, etc.) and reinforced by internet protocols (IPv6, 6LoWPAN, CoAP, etc.), IoT becomes a reality, with the goal of making things more aware, interactive, and efficient in order to create a safer and better world. As a result, any intelligent devices that can be addressed via a communication protocol is considered to be a part of the IoT [24]. The generic concept of IoT is depicted in Fig. 1.

Fig. 1: Generic Concept of IoT.

As a result, the concept of smart buildings was born. Various electronic equipment and applications are networked and communicate with one another in smart buildings. A large amount of data is generated in a system with a massive number of devices communicating with one another. Data management and analytics are expected to play a significant role in enhancing IoT-enabled smart buildings [25]. The following sections go over the fundamental characteristics and capabilities of smart buildings.

2.2 Smart Building

Smart Buildings are the next generation of buildings that must be allocated in Smart Cities because they integrate autonomy and adaptive control. Smart Buildings combine information technology, security, sustainable development, automation, industrial controllers, and communications to achieve maximum energy efficiency and user comfort [26-27].

The Smart Building is a structure whose features change over time. Smart buildings can respond to changes in the external and/or internal environment without requiring human intervention in order to provide comfort to occupants while also considering energy and financial perspectives [28]. It combines real-time tracking with event monitoring and data analytics to assist managers in optimizing available resources and improving reliability.

Some of the key characteristics of Smart Buildings are as follows [29]:

1) It improves performance and reliability in order to reduce energy consumption.
2) Analytical rules can be used to detect anomalies.
3) When a service is requested, real-time events can be centralized for correlation, consolidation, or to trigger a specific action.
4) Using captured data, energy analytics can be performed.
5) Less maintenance and management are needed, resulting in lower operating costs.
6) All metrics can be stored in a database for future use.
7) Develop scenarios for performing context awareness.
8) Conduct historical data analysis to detect trends and implement corrective actions.

Structures, research, systems, and technology all play a role in today's buildings. All of the elements that go into designing a building have improved over time as a result of technological advancements, research methods, and the tools available for designing a dependable and comfortable structure [30].

In order to construct a building, a number of regulations and rules that must be tracked. The establishment of a building requires a great deal of effort, research, and planning, but due to all of this extra work, we can now manage the environment within the building with the touch of a remote handheld. Not only that, but many organizations and governments have begun to consider the impact of buildings on the electrical grid as well as the environmental impact of these structures [31]. As a result, the construction of smart buildings is becoming increasingly popular. Smart buildings are structures with a large number of IoT sensors that continuously monitor the environment within the smart building and save this useful data on a server [32].

3. Key Applications In Smart Building

3.1 Energy Management

Because buildings consume 40% of total global energy, energy management in building is one of the most studied areas to date, not just in the development of smart buildings. A smart building, on the other hand, must not influence the level of service provided to users or residents of the building in order to accomplish this goal, which needs a solution that satisfies all parties. Commercial buildings already have energy management systems that optimize, monitor, and control the current energy consumption of the buildings [33]. These systems typically install non-intrusive meters on electric circuit to gather energy consumption data for building managers and users. Though, there is still a lot to be done at this point. Smart buildings require modification based on specific needs, which needs a certain level of knowledge. This means that the condition of the environment and the occupants is critical to the operation of smart building. For example, the Heating, Ventilation, and Air Conditioning (HVAC) system must be adjusted based on the number of people in the room, and the lighting system must adapt the lighting inside the building and track the intensity of light outside properly. IoT assists smart buildings in managing the consumption of energy from a macroeconomic point of view in terms of energy efficiency. As industry around the globe establishes goals to encourage this task, energy saving will become extremely important [34].

3.2 Localization

Building occupants and the environment can be controlled in real time by the availability of IoTs in commercial buildings. In this way, in different areas of the building we can have direct access to occupancy numbers and even find most users carrying a wireless device. This information can be used for a variety of Building Management System (BMS) applications in real time [35].

For example, real-time occupancy tracking in future smart building systems can intelligently control the HVAC to reduce energy consumption [36-37]. In addition to energy concerns, occupancy localization may aid in the rescue of people who survived in the event of an emergency [38].

It is difficult to determine occupancy when people are inside buildings. Current GPS technologies clearly do not have the accuracy needed inside buildings; they are mainly intended for area-based and geo-fencing services. Micro-location technologies, which enable any entity to be located with very high accuracy, usually up to a few centimetres, are a promising part of IoT [36].

Magnetic field mapping, Wireless Positioning Systems, Bluetooth Low Energy (BLE)-based Beacons/iBeacons, UWB-based Micro-location (Ultra-wide band), and RFID, are the five primary technologies in the market for IoT-based Micro-location [39].

3.3 Comfort

Like energy management and localization, occupant comfort is a main consideration of smart buildings in that the basic requirement of buildings is to establish comfortable living circumstances for building residents. Furthermore, because people spend typically 80% of their lives in buildings, a comfortable and healthy indoor environment is critical for occupant well-being and productivity. In real time, robust control and monitoring of the indoor built environment are required [40].

Future smart building systems, such as HVAC, will include numeric actuators and sensors, allowing the settings of temperature to be automatically configured. based on historical data and empirical learning, according to occupant needs and preferences. The implementation of these intelligent functions is based on an IoT system, which collects data, makes decisions, sends orders, and so on [34].

3.4 Automation

The core part of each smart building is BMS. It controls and monitors the building's mechanical and electrical equipment such as ventilation, lighting, power systems, fire systems, and security systems [41].

Pre-existing buildings, on the other hand, do not typically have these systems. In general, each type of configuration provides a unique list of options: HVAC controls climate, sensors and cameras provide security, and so on. Only when an energy management system is designed are the various subsystems related, but only through the building's energy management system [42].

3.5 Security

IoT security technologies are still in the early stages of development. The emergence of IoT has increased security concerns, and the reason for the decrease in safety is a lack of security system [43-44]. In contrast to the current Internet, IoT interaction patterns are frequently based on volatile and short connections between entities that lack a previously established trust link. However, given the distributed and dynamic nature of IoT, more flexible data sharing models are required, where some data can be shared with a group of entities or a set of unidentified recipients and, as a result, is not addressable a priori. Furthermore, due to the pervasive nature of the envisioned IoT scenarios, the manner in which this information is disseminated must take into account contextual data in which the sharing activity will be accomplished [45].

4. Communication Technologies

As shown in Fig. 2, IoT communication technologies connect heterogeneous objects to distribute specific smart services. In the presence of noisy and lossy communication links, IoT nodes should typically operate at low power. Examples of connectivity technologies used for the IoT in smart building are Bluetooth, WIFI, IEEE 802.15.4, Ethernet and Power Line Communication (PLC). Some specific communication technologies are also in use like UWB, NFC, and RFID. [46]. in the other hands, Multiple protocols are involved with IoT communication. Among them, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), IPv6 over Low power Wireless Personal Area Network (6LoWPAN), Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT) [47].

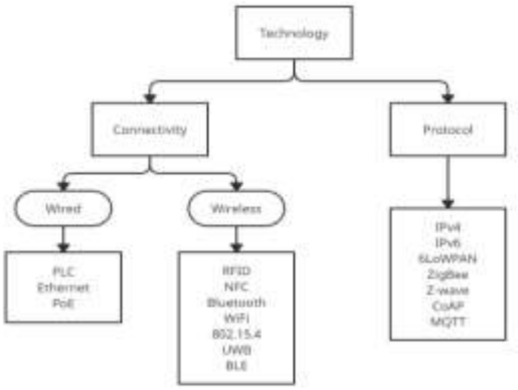

Fig. 2: IoT Smart Building Communication Technologies.

4.1 Connectivity

Ethernet and PLC are wired communication modes that can transmit data at a faster rate than other connectivity protocols. Wireless technologies such as WIFI, Bluetooth, and UWB, on the other hand, have superiority within the communication paradigm due to their greater flexibility [48]. According to the IEEE 802.11 standard [49], WIFI uses radio waves to communicate between devices. Short-range communication modes such as RFID, NFC, and Bluetooth are usually used to retrieve environmental data from physical devices. Table 1 demonstrates a brief summary associated to common communication technologies in use [50].

4.1.1 Power Line Communication (PLC):

PLC [51] technology exchanges data and information using existing power cables as a transmission medium.

PLC technology is regarded as one of the most cost-effective data communication solutions because of the advantages of free extra cabling. PLC technology has been widely adopted by automatic meter reading units [52], intelligent detection systems [53], and smart home solutions [54] at the heart of the smart grid concept. The introduction of new, more efficient digital signal processors, which enable the application of advanced modulation techniques, has opened up new possibilities for PLC technology [55].

PLC technology creates the potential for realizing the concept of the "smart city" and "smart home" where all domestic electronics are combined into a single centralized control network.

Table 1: IoT Smart Building Connectivity Technologies

Technology	Range	Frequency	Throughput	Power Consumption
PLC	100 m	baseband	> 1Mbps	---
Ethernet (PoE)	100 m	baseband	10 Mbps	100 W output
RFID	Up to 100 m	LF/HF/UHF/Microwave	Varies with frequency	Varies with frequency
NFC	10 cm	13.56 MHz	Up to 424 Kbps	< 15 mA
Bluetooth	100 m	2.4 GHz	2.1 Mbps	1 W Varies with class
802.15.4	< 100 m	2.4 GHz	0.25 Mbps	Varies with transiver
BLE	> 100 m	2.4 GHz	0.27 Mbps	0.5 W
WIFI (802.11.n)	75 m	2.4 and 5 GHz	600 Mbps	0.82 W
UWB	20 m	10.6 GHz	Up to 400 Mbps	100 mW

4.1.2 Power over Ethernet (PoE):

PoE is being used to fulfill a growing number of IoT requirements. By supplying a voltage to each pair of data conductors, DC power is conveyed. Because Ethernet uses differential signaling, adding a power signal has no effect on data transport. The following are the elements of a PoE system [56].

- Power Sourcing Equipment (PSE): Any equipment that permits power to be injected into a PoE network (mid-span or endspan). a mid-span PoE injector is an example of mid-span equipment (an Ethernet network energy provider). A PoE-enabled Ethernet switch is an example of end-span equipment;
- Powered Device (PD): Any end device that requires a PSE to function (e.g., a surveillance camera, wireless access point (WAP), and an IP phone,).

In smart building technologies, PoE has the potential to be a great success. The ability to supply both content device-supporting power and LAN-based transmission over the same connection is PoE's main feature. PoE's main benefit is the cost savings of an integrated infrastructure, which includes components and installation costs. it also eases the implementation of endpoint devices without the need for a high-voltage ac electric circuit [56].

While PoE has inherent data connectivity applications, it is also being considered for lighting and other applications. LEDs outperform older lighting technologies in terms of lumen output, and a PoE standard for 60 W is nearing completion (there also are proposals for the standardization for 95 W). PoE-based lighting goes beyond so-called "smart lighting" in that it provides a system that is linked to a centralized, software-based component that monitors all the actuators, sensors, and luminaries in a granular fashion, providing improved control and localized usage information that can be used for efficiency implementation (e.g., how many people are in the building at any given time and where they are located; how work spaces are used; natural lighting situations; and multibuilding/multifloor optimization). Retrofitting older lighting fixtures is relatively simple [56]. Fig. 3 depicts the various types of PoE.

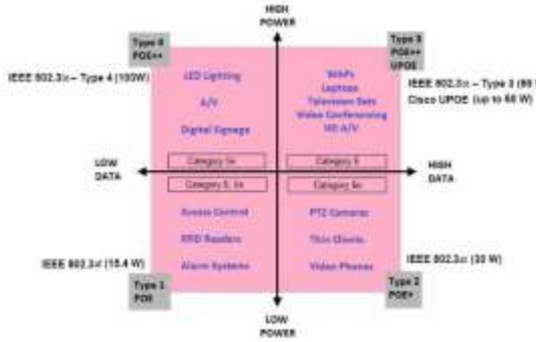

Fig. 3: Types of PoE [56].

4.1.3 Radio-Frequency Identification (RFID):

RFID is a noncontact communication technology which is used to track and identify objects without making physical contact. It allows data to be exchanged over short distances using radio signals [14, 57]. RFID reader, RFID tag, and antenna make up the RFID-based system [58]. A microchip attached to an antenna can be used as an RFID tag. Each RFID tag has its own unique identification number and is appended to an object. By querying the attached RFID tag through appropriate signals, an RFID reader can define an object and gain the corresponding information [59]. The signals between the RFID reader and the RFID tag are transmitted via an antenna. RFID has the following advantages over other technologies (low cost, small size, security, noncontact reading, large storage, reusability, durability, fast scanning, etc.) [60-61]. Because of these advantages, RFID can be used in the IoT perception layer to track and identify objects as well as exchange data.

RFID devices are generally divided into two types: active and passive. The passive RFID tags aren't powered by batteries. In reality, they communicate their data by utilizing the reader's interrogation signal. This type of tag is used in a wide range of applications. Particularly in the transportation industries, supply chain, and retail. They're also used as an access control mechanism in bank cards and road toll tags. Active RFID readers, on the other hand, have their own battery power and can initiate communication. Although radio coverage is more essential than passive tags, it comes at the cost of higher manufacturing costs. Indeed, one of the most intriguing benefits of RFID technology is its low cost, that would allow for widespread adoption. Active RFID tags could be used in hotels to provide automated check-in for customers, robotics in a smart home context, and port containers for cargo scanning, among other applications [62].

From a hardware perspective an RFID tag is a small microchip (e.g., 0.3mm × 0.3mm × 0.14mm) connected to an antenna that receives the reader signal and transmits the tag identity. The tag comes in an attached sticker package [63].

4.1.4 Near-Field Communication (NFC):

NFC is a group of communication protocols that allows two devices up to a distance of 10 cm to communicate with each other. When it comes to mobility, one device should be considered portable to facilitate the right proximity. Passive NFC tags can be read by all NFC-enabled devices, which allows them to transfer information and act as a smart card to perform transactions. As such, NFC may be described as a tool for communication and identification [64].

4.1.5 Bluetooth:

Bluetooth is also another wireless communication technique that lets data to be transferred between nodes over short distances. It was developed by the Ericsson telecommunications company to solve the issue of data synchronization. Bluetooth Special Interest Group (SIG) now manages and maintains it, with the most recent version of Bluetooth 5 from the most recent announcement. Bluetooth is appropriate for smaller devices such as personal computers, media players, speakers, phones, and so on [65].

4.1.6 IEEE 802.15.4:

The IEEE 802.15.4 protocol was developed to specify a physical layer (PHY) and a MAC sub-layer for low-rate wireless private area networks (LR-WPAN) [66]. It is also used by WSNs, M2M, and IoT due to its specifications such as high message throughput, low cost, low data rate, and low power consumption. It offers the ability to handle a large number of nodes. platform compatibility, and dependable communication. also, it offers advanced authentication, encryption, and security services. It does not, however, provide QoS guarantee [12].

Each 802.15.4-based channel is 2 MHz wide and separated by 5 MHz from the other channels. To prevent channels from interfering with one another, this rule is implemented. This protocol can support mesh and star topologies (not limited to just those two).

Several protocols such as ZigBee and WirelessHART [67] have been built on top of the IEEE 802.15.4, all to be as resource-efficient as possible. Also, as the number of IoT devices continues to grow, a growing number of them are made as IEEE 802.15.4-compliant devices.

4.1.7 Bluetooth Low-Energy (BLE):

Due to its ultra-low power consumption and lower latency than traditional Bluetooth, BLE is a promising technology in the IoT space. The BLE operates on a client-server model, with a client connecting to and accessing one or more servers [50]. In comparison to previous versions, BLE or Bluetooth Smart uses a short-range radio with a low power consumption to operate for longer periods of time (even years). Its range (roughly 100 meters) is ten times that of traditional Bluetooth, and its latency is 15 times lower [68]. BLE transmits at powers between 0.01 microwatts (mW) to 10 microwatts (mW). BLE is supported by most smartphone manufacturers and is now found in most smartphones. Vehicle-to-vehicle communications [69] and wireless sensor networks [70] have both proven feasible. BLE uses less energy and transmits with a higher transmission energy to data bit ratio (MTT: transmit energy to data bit ratio) than ZigBee [71].

4.1.8 WIFI:

WIFI is a communication technology based on the IEEE 802.11 standards that uses radio waves for local area networking among devices. The most commonly used frequencies are the 5.8 GHz SHF and 2.4 GHz UHF ISM radio bands. it is already popularly used in smart TVs, tablets, smartphones, personal computers and a variety of other everyday devices. One of the benefits of WIFI is that any device within a wireless modem range can try to connect to the network. However, this is also a weakness due to security concerns, as it is more exposed to attack than a wired cable connections [65].

4.1.9 Ultra-Wide Band (UWB):

In comparison to WIFI technologies, UWB has a lower power consumption, higher bandwidth, but a shorter range. They are also inexpensive. However, they keep consuming a considerable amount of power from battery-limited devices such as smartphones, so micro-location services must account for this [39].

4.2 Protocols

When it comes to the IoT, standards and protocols are often overlooked. Communication is often at the top of the list of the industry's focus. While communication between servers, gateways, sensors, devices, and user applications is critical to the IoT, it would be impossible without the right IoT protocols.

4.2.1 IPv6:

Because the 32-bit address space provided by IPv4 has been depleted and is no longer capable of delivering each device with a unique address, IPv6 is a key component of the IoT. IPv6's 128-bit address space provides the necessary infrastructure to host billions of IoT devices. IPv6 assigns an IP address to each device for identification. It enables end devices to have globally valid IP addresses, direct end-to-end interactions and security even without an overlay network, which is needed for peer-to-peer networks with peers in local IPv4 networks [72].

4.2.2 Low-Power Wireless Personal Area Network (6LoWPAN): 6LoWPAN is another IETF protocol that operates in the network layer of the infrastructure. Because 6LoWPAN has been built using IPv6 as a base, interoperability with other IP networks and other IEEE 802.15.4 wireless devices is facilitated. 6LoWPAN allows uniquely access to each constrained device in the network, simplifying management tasks [73].

6LoWPAN uses datagrams IPv6 compression header techniques. The space available for packages IPv6 encapsulate in 802.15.4 frames is the motivation of compression techniques. 6LoWPAN defines compression-based encoding formats based on common state in contexts. In other words, it uses fields which are known implicitly to all network nodes or which can be deduced from the MAC layer [74].

Due to its low energy consumption and low cost, 6LoWPAN is IoT-friendly, which incorporates a large number of low-cost devices. 6LoWPAN has several advantages including high connectivity, legacy architectures compatibility, ad hoc self-organization, and so on [75].

4.2.3Constrained Application Protocol (CoAP):

Due to its complexity, HTTP cannot be used in IoT. To solve the problem, CoAP was proposed as a way to modify some HTTP functions to fulfill IoT requirements. CoAP is the application layer protocol in the 6LoWPAN protocol stack, and it aims to allow devices with limited resources to engage in RESTful interactions. CoAP supports push notifications and group communication, but not broadcasting [76]. CoAP provides important features such as HTTP interaction, resource discovery, block-wise resource transport, resource observation, and security [77].

The overall CoAP protocol functionality is shown in Fig. 4 [12].

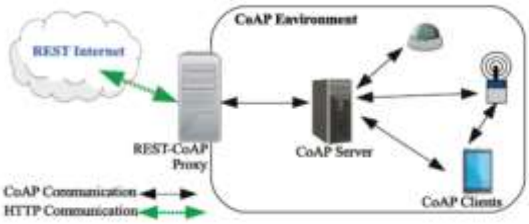

Fig. 4: Functionality of CoAP [12].

4.2.4 MQTT:

MQTT is a lightweight and simple protocol that supports low bandwidth and high latency networks [75]. MQTT's ability to adapt for verity platforms to link things to the Internet is one of its advantages [65]. MQTT can thus be used as a messaging protocol between servers, sensors, and actuators, making it an important component of the IoT [75].

MQTT is best suited for low-bandwidth or unreliable networks with constrained devices. A subscriber, broker, and publisher are the three components of MQTT. A device must be registered for a specific topic before it can become a subscriber. After that, the publisher creates content and distributes it to subscribers through brokers. QoS is determined by MQTT based on the message delivery reliability. It assigns a value to QoS based on one of three predefined levels [78].

The architecture of publish/subscribe as depicted in Fig. 5 [12].

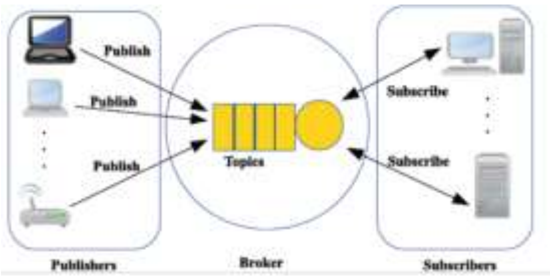

Fig. 5: MQTT Architecture [12]

4.2.5 Zigbee:

Zigbee is an IEEE 802.15.4-based standard for low-power, short-range communications [65]. ZigBee is self-healing, self-forming, and supports star and mesh topologies, which makes it similar to IEEE 802.15.4 [79-80]. It defines the architecture's upper layers on top of the IEEE 802.15.4 standard's PHY and MAC layers. The ZigBee protocol is designed specifically for control and monitoring applications. As a result, it's appropriate for applications like lighting, industrial control, personal health care, building automation, and commercial control [50].

Zigbee is commonly used for localization in wireless sensor networks due to its low power requirements. Among IoT devices, though, it is not popular due to the extra hardware that is needed [81].

4.2.6 Z-Wave:

Z-wave is a short-range wireless connection with high reliability low energy consumption, and low costs, [82]. The primary goal of Z-wave is providing reliable communication between a control unit and one or more end-devices, Z-wave is appropriate for low-bandwidth networks. Note that there can be no greater than 232 nodes (slaves) in the Z-Wave network, and that all of these nodes (slaves) are controlled by the controller and have routing capability [82, 61]. Z-wave network supports dynamic routing technology and stores a route list in the controller's memory for each slave [83]. Although both Z-wave and ZigBee support low-energy and low-cost short-range wireless communication, there are some differences between them. The frequency band in which the physical layer operates is the major difference between ZigBee and Z-wave. In ZigBee, the physical layer's frequency band is typically 2.4 GHz, whereas in Z-wave, the frequency band is less than 1 GHz. The ZigBee network can support up to 65000 end devices (slaves), whereas the Z-wave network can only support 232 [61]. When compared to the ZigBee architecture, Z-wave is much easier to implement.

4.3 Network Topologies:

A network's topology is a geometric description of the relationship between all of the links and linking devices (often referred to as nodes). mesh, star, bus, and tree are the four basic topologies that can be used.

4.3.1 Bus Topology:

The topology of the bus was one of the first topologies used in the development of early local networks. It is a kind of multipoint connection in which a long cable serves as a backbone to connect all network devices. Nodes are connected by drop lines and taps to the bus cable. A drop line is a connection between the main cable and the device. A tap is a connector that splits into the main cable or punctures a cable sheathing to establish a touch with the metallic core.

The ease of installation is one of the benefits of a bus topology. Furthermore, compared to other topologies, a bus uses less cabling. Disadvantages, on the other hand, include difficult fault isolation and reconnection. A bus is usually designed to be as efficient as possible when it is installed. As a result, adding new devices can be difficult. Signal reflection at the taps can also degrade the quality of the signal. Furthermore, even between devices on the same side of the problem, a fault or break in the bus cable stops all transmission [84].

4.3.2 Star Topology:

Unlike bus topology, star topology has a point-to-point connection to a central device called a hub. The devices are not directly connected to one another. If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device. One of the important advantages of star topology in robustness (If one link fails, only that link is affected). The topology of stars is easy fault isolation as long as the hub works, but the whole system will fail if the hub goes down [84].

4.3.2 Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device. Compared to other network topologies, a mesh has several advantages. First, using dedicated links ensures that each connection can hold its own data load, avoiding traffic congestion that can happen when multiple devices share a single link. Second, a mesh topology is extremely durable. If one link fails, the system as a whole does not become unusable. Finally, there's the benefit of security or privacy. Only the intended recipient sees each message when it travels along a dedicated line.

The main drawbacks of a mesh are the amount of wiring or frequencies required, as well as the number of I/O ports required. First, installation and reconnection are difficult because every device must be connected to every other device. Second, the sheer bulk of the wiring may be greater than the space available (in floors, ceilings, or walls,). Finally, the hardware (I/O ports and cables) required to connect each link can be prohibitively expensive [84].

4.3.4 Tree Topology:

Tree Network Topology is made either from subordinating a set of star network topologies to a central node or from linking a set of star network topologies directly via a bus so that the functionality of the central node is distributed among various high level star network topology nodes. One of the main advantages of the Tree Network Topology is the ability to expand the network. Expansion can be as easy as linking a further star network topology to a bus.

One of the advantages of tree topology is providing a hierarchical as well as central data arrangement of the nodes and this allow more scalability in adding new devices easily. The disadvantage of tree topology is the dense network traffic as data travels form the central node. Also, it requires large number of cables or frequencies than star topology [85].

4.4 Network Types/Size:

After the definition of networks and discussion of their physical structures in the previous section, we need to discuss various areas of networks we meet in today's world.

4.4.1 Personal Area Network (PAN):

PAN is a computer network that links electronic devices in a single person's office. [86] A PAN is a network that lets data to be sent between devices like tablets, smartphones, computers, and personal digital assistants. PANs can be used to communicate between personal devices or to connect to a higher-level network and the Internet, with one master device acting as the gateway. A PAN can be wireless or run over wired connections like USB. A wireless personal area network (WPAN) is a PAN that uses a low-power, short-range wireless network technology like Bluetooth, IrDA, or ZigBee to communicate. A WPAN's range is between a few centimeters and a few meters [86].

4.4.2 Local Area Network (LAN): LAN is typically owned by a single company and connects several hosts in a single office, building, or faculty. A LAN can be as simple as two PCs and a printer in someone's home office, or it can strengthen throughout a corporation and include video and audio devices, depending on the needs of an organization. Each host in a LAN has a unique identifier, called an address. A packet sent from one host to another contains both the source and destination hosts' addresses. When LANs were used in isolation (which is rare nowadays), they were designed to allow hosts to share resources [84].

4.4.3 Wide Area Network (WAN):

WAN is a network that connects devices that are capable of communicating with one another. WAN has a greater geographical reach than LAN, and can connect multiple locations within a city, a state, a country, or even the entire world. A local area network (LAN) connects hosts, whereas a wide area network (WAN) uses connecting devices such as routers, and modems. As opposed to a LAN, which is typically owned by the organization that utilizes it, a WAN is typically created and maintained by communication companies and leased by the organization that utilizes it [84].

5. Survey

In this section, the survey of many researches in term of key application (discussed in section 3) of IoT smart building are presented. The survey is based on communication and network technologies.

5.1 Energy:

In [87], the authors proposed a user interface for creating simple energy-awareness rules on top of their RESTful architecture. They presented an IP-based WSN where nodes send data using Web services. The authors showed that the implemented method is doable for resource-constrained sensor nodes in terms of acquisition time for the sensor data and power consumption. They used 802.15.4 as the physical layer standard. The 6LoWPAN is used as a transmission protocol in their proposed architecture. The sensor nodes were connected to a mesh topology. Their proposed architecture was designed to work on a LAN with the existence of a central monitoring server. Furthermore, they demonstrated that TCP can be supported in specific network configurations.

Pan et al. [88] studied the statistical relationship between the energy use of cooling and heating, environmental factors/occupancy status and total energy use. The authors created a framework for automated energy control based on location. The framework uses a cellphone with GPS location sensors to locate the user. WIFI is used as the connectivity standard in home/office buildings. The location is received in the building by IPv4 through Network Address Translation (NAT), so the area of the network is the WAN. The network is connected to a star topology with a central web server. The system calculates the distance between the mobile device and the destination building using map data, and if the distance is less than a certain threshold, the energy policy plan will be updated. They used simulated scenarios and electricity meters to demonstrate the effectiveness of the IoT-based framework.

Balsamo et al [89] presented an innovative energy-neutral and nonintrusive Wireless Energy Meter (NIWEM) to measure current, voltage and power factor. Among its key features, the NIWEM is completely noninvasive and it can self-sustain its operations by harvesting energy from the monitored load. They used IEEE 802.15.4/Zigbee as a communication technology for connecting and transmitting the measured power consumption between the energy meter and a Gateway that is connected to a java-enabled host. The star topology was used as the connected network while the size of the network is LAN.

Plageras et al. [90] proposed a monitoring system for smart buildings based on IoT sensors. The proposed system was tested in a simulation environment. They used WIFI as the connectivity technology in the building environment and 6LoWPAN was used as the transmission protocol. The results demonstrated that by combining several IoT-based sensors, a better monitoring system in a smart building can be achieved. The scale of the network implemented is a LAN. The implemented topology was a hybrid that relied on both star and mesh networks, and they concluded that the mesh topology provides greater fault tolerance. It is expected that the proposed system will increase energy efficiency and enabling green and smart buildings.

Other methods use communication networks to transfer context information to LED lighting controllers is by using PLC as a communication technology, which reduces the need for extra wired systems and takes advantage of the present infrastructure. The authors of [91] proposed a novel interfacing technique coupling diversity has the potential to mitigate this threat. They investigated the impact of power line topology, distance and voltage on the circuits. The type of topology implemented was a bus. The measurement is transmitted over a LAN. In this case, the controllers and sensors are energized directly from the power grid, removing other backup sources used in WSN system.

Another kind of network sensor communication is PoE which takes benefit of technology advance that enables electronic device to be energized through internet wire in a building. The author of [92] proposed smart LED energy consumption systems using a combination of solar and LED lighting with PoE. The devices, in this case, have an RJ45 port which allows both communications between elements of the data network using the TCP/IP protocol to have an intelligent information network for controllers and sensors in an environment. Mesh topology is used in an office of 100 m2 to connect the network (LAN).

The authors of [93] discussed the possibility of creating a self-powered industrial sensor network. The system is composed of sensing nodes that operate on a battery plus energy harvested from the environment. The network is composed of clusters with a star topology where resources and channel access are coordinated by a central access point (AP). The UWB based WSN was used as the connectivity protocol. The area of the implemented network is the LAN. They concluded that UWB can act as an enabler to significantly extend the lifetime of wireless sensor networks.

5.2 Localization

In [38], data from APs is combined with sensors and cloud-based calendars to predict the occupancy of buildings for emergency response purposes. WIFI is used as a standard for device connectivity. The building was divided into zones connected by a star topology. SNORT, an intrusion detection tool, was used to analyze HTTP traffic and identify mobile devices connected via IPv4 addresses. Once a device's MAC address has been determined, the AP to which it is connected is used to determine the mobile device's zone. This data is then combined with sensors and room schedules to produce an estimate of the building's occupancy. The size of the network is a WAN in which a Google cloud-based database is used to store the occupants of a building.

Conte et al. [94] proposed occupancy detection via the use of the iBeacon protocol based on Bluetooth available on smart devices. The system was built upon low-cost Bluetooth antennas and a client mobile application installed on the occupants' smartphones. They modified the iBeacon protocol to make it more accurate and efficient for occupancy detection to classify occupants into different rooms based on the received signal strength indicators (RSSIs) from different iBeacons. They are used in conjunction with and contrasted with two connectivity standards: WIFI and Bluetooth. They concluded that WIFI is more reliable and stable, but it requires them to keep a high-power wireless adapter. They saved about 15% of their energy using the Bluetooth-based architecture. The devices in the network are connected in a star topology and the area of the network is PAN.

Alletto et al. [95] presented a system of location-aware for an IoT-based museum that acts as a smart tourist guide. The visitor is given a wearable device that combines location awareness abilities and image recognition. The system's connectivity standards are WIFI and BLE. When a visitor arrives at a location with specific artwork or historical significance, the wearable device uses a BLE infrastructure to track the user and then sends data to the cloud via a WIFI AP. The processing center uses the data to interact with the visitor and offer them with interesting content. The network's topology is a star. The network can operate in both PAN and WAN modes, with the system interacting with the cloud to store multimedia content created by the user and to share events generated by the environment on the user's social network.

The authors of [96] proposed a system for locating people inside a smart building. Several services are provided to the residents of this building, including solutions to energy consumption issues. Also, they used RFID with IR as the connectivity standard to give solutions to localization requirements. Thus, imprecise location estimates due to RFID signal variations in indoor environments can be improved since IR is a non-RF based technology, and therefore, it is not influenced by the losses through reflection, diffraction or absorption in walls, floors, etc. of the building, which affect RF signals in indoor environments. The network is a WAN in which the actuators and sensors deployed can be remotely controlled via the Internet, allowing for a wide range of control and monitoring applications. The IRs are connected to a single RFID reader in a star topology. Finally, the estimation results produced are highly accurate for the user's location data. As a result, they offer a low-cost option for ambient adaptation based on human presence.

5.3 Comfort

Kelly et al. [97] developed an IoT system for monitoring utility usage and indoor environmental conditions in residential buildings. This system used ZigBee to establish the sensing network, which consisted of XBee-S2 modules, as well as a gateway to bridge the data transition between ZigBee and IPv6. The end devices collect and forward data to a coordinator and then the ZigBee protocol data format is translated to the IPV6 format. The combination of star and mesh topologies is implemented in the system and the scale of the network is specified to be a WAN. The primary contribution to this system is the proof of the ability to connect with Zigbee and IPv6, so a low-cost flexible system is available to integrate IoT with home monitoring systems to determine the wellness of residents.

In [98], The authors reported on monitoring indoor air quality by detecting pollutant levels for indoor environments, health and comfort of individuals. The network is made up of end device sensors equipped with photoionization detectors, routers that allow the network to be propagated over long distances, and a coordinator that interacts with a computer. The implantation is based on ZigBee as the communication protocol. The nodes are connected as a mesh network. The size of the implemented system is a LAN in which the data is stored and managed in a local SQLite database. They found that ZigBee-based WSNs are especially suitable for indoor air quality surveillance because wired deployment is costly and inefficient.

Kodali and Sarjerao [99] suggested IoT-based applications for urban climate monitoring. A carbon monoxide sensor is used to detect carbon monoxide levels in the air, and a sharp dust sensor is used to measure smoke and particulates in the environment. The proposed pollution monitoring system is based on WIFI as the connectivity technology between the sensors and the server. MQTT is used as a transmission protocol. The sensors are connected to the gateway in the star network. By using a mobile application in WAN, the subscriber can view the polluted content on this system.

Using low-cost sensors, Anindya et al [100] developed a real-time method to check parameters of Indoor Air Quality (IAQ), such as dust CO2. Humidity and temperature between the sensor nodes, they used WIFI as the connectivity standard. They implemented this system in the campus (LAN) area, using MQTT as a communication protocol. The results of the prototype design have been implemented, with three sensor nodes installed and tested at the campus sampling location. The sensor node circuit is made up of a microcontroller MCU ESP8266 module with wireless WIFI communication systems and is connected to the gateway in a star topology. They came to the conclusion that the proposed prototype could collect data more efficiently and quickly.

5.4 Automation

In the paper [101], the authors designed and implemented an open and efficient Prototype System to solve the problem of costly BMS, consisting of heterogeneous, small-scale wireless devices. They used CoAP protocol to integrate devices with different hardware. Their solution addresses sensors and actuators that communicate via IPv4, IPv6 or Zigbee protocols and are used for data exchange. They also propose and implement a mechanism for automatically setting up wireless devices and detecting their detection capabilities. The topology of the network is heterogeneous and can be controlled by the internet WAN. The detected devices are then reported to the network through a gateway that allows other nodes in the network to access the devices.

Authors in [102] provided a comparative analysis of ZigBee topologies for wireless lighting automation systems. The implemented topologies are star, mesh and tree. Two WSN routing protocols, AODV and DSR, are used to test these topologies. The comparison shows that the end-to-end delay is minimal when DSR is implemented in a star topology. It does, however, have a problem with the central point of failure. If the system is not time-critical, however, a mesh topology with the same routing protocol has emerged as a promising solution. The area of the network is LAN.

Also, Khanchuea et al [103] developed an IoT gateway. This gateway was created using the ESP32 card. With this platform, a mesh-type WIFI network is established to exchange information with a network of sensors. The sensor nodes use the DHT22 sensor to record temperature and humidity values. These nodes establish a ZigBee network to send the sensed data to a router node. This router node takes the data received by ZigBee and is relayed via WIFI to the gateway node. Although in this system there is a co-existence of two wireless networks (one ZigBee and another WIFI), the gateway node only establishes WIFI connections, so it is empty. The nodes are connected to a tree-based wireless network to coexist with the ZigBee mesh networks. The MQTT is used for message delivery and protocol conversion. Also, the BLE features of the ESP32 chip are used to help in the process of self-organizing a wireless network. The size of the network is a LAN.

Table 2: Summary of the Surveyed Researches

Application	Ref.	Connectivity and Transmission	Network Topology	Network Size
Energy	[87]	802.15.4, 6LoWPAN	Mesh	LAN
	[88]	WiFi, IPv4 (NAT)	Star	WAN
	[89]	802.15.4, ZigBee	Star	LAN
	[90]	WiFi, 6LoWPAN	Star, Mesh	LAN
	[91]	PLC	Bus	LAN
	[92]	PoE	Mesh	LAN
	[93]	UWB	Star	LAN
Localization	[38]	WiFi, IPv4	Star	WAN
	[94]	Bluetooth, WiFi	Star	PAN
	[95]	BLE, WiFi	Star	PAN, WAN
	[96]	RFID	Star	WAN
Comfort	[97]	Zigbee, IPv6	Star, Mesh	WAN
	[98]	Zigbee	Mesh	LAN
	[99]	WiFi, MQTT	Star	WAN
	[100]	WiFi, MQTT	Star	LAN
Automation	[101]	CoAP	Heterogeneous	WAN
	[102]	ZigBee	Star, Mesh	LAN
	[103]	WiFi, BLE, ZigBee, MQTT	Tree	LAN
Security	[104]	ZigBee	Mesh	PAN
	[105]	Z-wave	Mesh	PAN
	[106]	ZigBee, MQTT	Star	WAN

5.5 Security

Morgner et al. [104] described a set of attacks based on Zigbee protocol flaws. The attacks were separated into two groups: These require access to the Zigbee light link master key (command injection, network key extraction and hijack) and do not require the use of cryptographic protocols (DoS, reset and blink). Popular lighting models such as Ethernet GE Link, Osram Lightify and Philips Hue connected to a mesh topology were among the target systems. Their goal was to show a series of attacks against the Zigbee protocol by exploiting the protocol's master key vulnerability and the unprotected frames used for communication between different PANs.

The authors of [105] discussed the security features of two IoT protocols, Z-Wave and Thread. They discussed the physical security authentication, trust, authorization, data integrity, confidentiality, and privacy issues that IoT presents. Some well-known IoT attacks include third-party attacks, replay attacks, man-in-the-middle (MITM) attacks, and distributed denial of service (DDoS). They used mesh topology to connect network devices. The network's size is PAN. They also investigated the Z-Wave and Thread authentication processes.

The [106] includes a preliminary performance analysis in which an IoT application framework based on fog computing principles is integrated with MQTT and user managed access (UMA). Despite the fact that such approaches are concerned with end-to-end secure communications, authorization, and authentication, little attention is paid to how information is effectively shared once acquired by IoT platforms. In the implemented system, each IoT device is equipped with a Zigbee device. The devices are connected to a star topology. The implementation area has been expanded to include the WAN. The model proposed should increase the security level of small to large scale IoT applications in smart cities or smart building applications. Table 2 shows the summary of these researches.

6. Conclusion

As advanced technologies continue to develop and become more integrated into our lives, they have opened up new possibilities for enhancing the service's performance in buildings, cities, and communities. This paper has explored the current existing research and future potentials of the IoT in the context of the envisioned goals of smart buildings, focusing on one important part of the design. In this paper, the area of smart building with a special focus on the role of communication technologies used in a number of important applications were surveyed.

References

[1] D. Evans,. The internet of things: How the next evolution of the internet is changing everything, CISCO white paper, pp.1-11 .2011.
[2] M. R. Bashir, Model driven big data analytics framework for IoT enabled smart buildings: A systematic literature review, Intellisys, 2017.
[3] M. M. Rathore, A. Ahmad, A. Paul and S. Rho, Urban planning and building smart cities based on the internet of things using big data analytics, Computer Networks, Vol.101, pp.63-80, 2016.
[4] J. Shah and M. Mishra, Customized IoT enabled wireless sensing and monitoring platform for smart buildings, Procedia Technology, Vol.23, pp.256-263, 2016.
[5] D. Clements-Croome, Intelligent buildings: an introduction, Routledge, 2013.
[6] J. Sinopoli, Smart buildings: a handbook for the design and operation of building technology systems, Spicewood Publishing 2006.
[7] M. Batty, Smart cities, big data, Environment and Planning B: Planning and Design, Vol.39, pp. 191-193, 2012.
[8] M. R. Palattella, N. Accettura and X. Vilajosana, Standardized protocol stack for the internet of (important) things, IEEE communications surveys & tutorials, Vol.15, No.3 pp. 1389-1406, 2012.
[9] F. Montesi, JOLIE: a Service-oriented programming language, Master's thesis, University of Bologna, 2010.
[10] K. Khanda, D, Salikhov, K, Gusmanov, M. Mazzara and N. Mavridis, Microservice-based IoT for smart buildings, IEEE 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp.305-308, 2017.
[11] L. Atzori, A. Iera and G. Morabito, The internet of things: A survey, Computer networks, Vol.54, No.15 pp.2787-2805 2010.
[12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE communications surveys & tutorials, Vol.17, No.4, pp.2347-2376, 2015.
[13] R. Khan, S. U. Khan, R. Zaheer and S. Khan, Future internet: the internet of things architecture, possible applications and key challenges, IEEE 10th international conference on frontiers of information technology, pp. 257–260, 2012.

[14] I. Andrea, C. Chrysostomou and G. Hadjichristofi, Internet of Things: Security vulnerabilities and challenges, IEEE symposium on computers and communication (ISCC), pp. 180–187, 2015.

[15] P. López, D. Fernández, A. J. Jara and A. F. Skarmeta, Survey of internet of things technologies for clinical environments, IEEE 27th International Conference on Advanced Information Networking and Applications Workshops, pp.1349–1354, 2013.

[16] D, Yi and D Liang, A survey of the internet of things, Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010), Atlantis Press, pp.358–366, 2010.

[17] A. Gluhak, et al. A survey on facilities for experimental internet of things research. IEEE Communications Magazine, Vol.49, No.11, pp.58-67, 2011.

[18] Z. Sheng, et al. A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities, IEEE wireless communications, Vol.20, no.6, pp.91–98, 2013.

[19] K. Ashton, That 'internet of things' thing, RFID journal, Vol.22, No.7, pp.97-114, 2009.

[20] T. Goetz, Harnessing the power of feedback loops, Wired magazine, Vol.19 No.7, 2011.

[21] J. Manyika, et al. Disruptive technologies: Advances that will transform life, business, and the global economy, San Francisco, CA McKinsey Global Institute, Vol.180. 2013.

[22] M. Dohler, Machine-to-machine technologies, applications & markets, IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), 2013.

[23] I. Peña-López, ITU Internet report 2005: the internet of things, 2005.

[24] B. S. Brad and M. M. Murar, Smart buildings using IoT technologies, Constructions of Unique Buildings and Structures, Vol.5, No.20, pp.15-27, 2014.

[25] M. R. Bashir, A. Q. Gill, IoT enabled smart buildings: A systematic review, IEEE Intelligent Systems Conference (IntelliSys), pp.151–159, 2017.

[26] A. H. Buckman, M. Mayfield and S. B. M. Beck, What is a smart building?, Smart and Sustainable Built Environment, Vol.3 No.2 pp.92–109, 2014.

[27] Z. Wang, L. Wang, A. I. Dounis and R. Yang, Multi-agent control system with information fusion based comfort model for smart buildings, Applied Energy, Vol.99, pp.247-254, 2012.

[28] A. Harris, Smart buildings, Engineering and Technology, Vol.7, No.6, pp.52-54, 2012.

[29] E. Carrillo, V. Benitez, C. Mendoza, J. Pacheco, IoT framework for smart buildings with cloud computing, IEEE First International Smart Cities Conference (ISC2), pp.1-6, 2015.

[30] M. R. Bashir and A. Q. Gi, Towards an IoT big data analytics framework: smart buildings systems, IEEE 18th International Conference on High Performance Computing and Communications, IEEE 14th International Conference on Smart City, IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp.1325-1332, 2016.

[31] D. J. Leeds, The soft grid 2013-2020: Big data & utility analytics for smart grid, GTM Research, 2012.

[32] S. Kejriwal and S. Mahajan Smart buildings: How IoT technology aims to add value for real estate companies, Deloitte Center for Financial Services, 2016 .

[33] L. Karim, A. Boulmakoul and A. Lbath, Real time analytics of urban congestion trajectories on Hadoop-MongoDB cloud ecosystem, the second International Conference on Internet of Things, Data and Cloud Computing (ICC), At Cambridge city, Churchill College. University of Cambridge, United Kingdom. ACM Digital Library. ISBN: 978-1-4503-4774-7, 2017.

[34] A. Daissaoui, A. Boulmakoul, L. Karim and A. Lbath, IoT and big data analytics for smart buildings: A survey, Procedia Computer Science, Vol.170, pp.161-168, 2020.

[35] K. Akkaya, I. Guvenc, R. Aygun, N. Pala and A. Kadri, IoT-based occupancy monitoring techniques for energy-efficient smart buildings, IEEE Wireless communications and networking conference workshops (WCNCW), pp.58-63, 2015.

[36] Al. De Paola, M. Ortolani, G. Lo Re, G. Anastasi and S. K. Das Intelligent management systems for energy efficiency in buildings: A survey, ACM Computing Surveys (CSUR), Vol.47, No.1, pp.13:1–13:38, 2014.

[37] T. A. Nguyen and M. Aiello, Energy intelligent buildings based on user activity: A survey, Energy and buildings, Vol.56. pp. 244-257, 2013.

[38] K. Nyarko and C. Wright-Brown, Cloud based passive building occupancy characterization for attack and disaster response, IEEE International Conference on Technologies for Homeland Security (HST), pp.748– 753, 2013.

[39] F. Zafari, I. Papapanagiotou and K. Christidis, Microlocation for internet-of-things-equipped smart buildings, IEEE Internet of Things Journal, Vol.3, No.1, pp. 96-112, 2015.

[40] R. Yang and L. Wang, Multi-agent based energy and comfort management in a building environment considering behaviors of occupants, IEEE Power and Energy Society General Meeting, pp.1-7, 2012.

[41] The Internet of Things in Smart Buildings 2014 to 2020, Memoori Business Intelligence Ltd, 2014.

[42] F. J. Ferrández-Pastor, H. Mora, A. Jimeno-Morenilla and B. Volckaert, Deployment of IoT edge and fog computing technologies to develop smart building services, Sustainability, Vol.10, No.11, p.3832, 2018.

[43] Y. Jie, J. Y. Pei, L. Jun, G. Yun and X. Wei, Smart home system based on iot technologies, IEEE

International conference on computational and information sciences, pp.1789–1791, 2013.

[44] X. Yuan, S. Peng, A research on secure smart home based on the internet of things, IEEE International Conference on Information Science and Technology, pp.737–740, 2012.

[45] J. L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé, D. G. Carrillo and A. F. Skarmeta, SAFIR: Secure access framework for IoT-enabled services on smart buildingsm, Journal of Computer and System Sciences, Vol.81. issie.8, pp. 1452-1463, 2015.

[46] Y. Zhang, K. Yang and H. Chen, An adaptive MAC layer energy-Saving algorithm for ZigBee-Enabled IoT networks, International Conference on Smart City and Informatization. Springer, Singapore, 2019.

[47] S. Schneide, Understanding the protocols behind the internet of things, Electronic design, Vol.9, No.10, 2013.

[48] E. Borgia, The Internet of Things vision: Key features, applications and open issues, Computer Communications, Vol.54 pp.1-31, 2014.

[49] E. Ferro and F. Potort, Bluetooth and Wi-Fi wireless protocols: a survey and a comparison, IEEE Wireless Communications, Vol.12, No.1, pp. 12-26, 2005.

[50] B. N. Silva, M. Khan and K. Han, Internet of things: A comprehensive review of enabling technologies, architecture, and challenges, IETE Technical review, Vol.35, No.2, pp.205-220, 2018.

[51] H. C. Ferreira, L. Lampe, J. Newbury and T. G. Swart, Power line communications: theory and applications for narrowband and broadband communications over power lines, John Wiley & Sons, 2011.

[52] M. Choi, S. Ju and Y. Lim, Design of integrated meter reading system based on power-line communication, IEEE International Symposium on Power Line Communications and Its Applications, pp.280-284., 2008.

[53] F. J. Sánchez-Pacheco, P. J. Sotorrío-Ruiz, J. R. Heredia-Larrubia, F, Pérez-Hidalgom and M, Sidrach, PLC-based PV plants smart monitoring system: field measurements and uncertainty estimation, IEEE Transactions on instrumentation and measurement, Vol.63, No.9, pp. 2215-222, 2014.

[54] M. Li and H. J. Lin, Design and implementation of smart home control systems based on wireless sensor networks and power line communications, IEEE Transactions on Industrial Electronics, Vol.62, No.7, pp. 4430-4442, 2014.

[55] A. A. Zhilenkov, D. D. Gilyazov, I. I. Matveev and Y. V. Krishtal, Power line communication in IoT-systems, IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp.242-245, 2017.

[56] D. Minoli, K. Sohraby and B. Occhiogrosso, IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems, IEEE Internet of Things Journal, Vol.4, No.1, 2017.

[57] K. Zhao and L. Ge A survey on the internet of things security, IEEE Ninth international conference on computational intelligence and security, pp.663–667, 2013.

[58] K. Finkenzeller, RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, John wiley & sons, 2010.

[59] S. Lahiri, R. F. I. D. Sourcebook, IBM press, Upper Saddle River, NJ, USA 2005.

[60] D. Ćika, M. Draganić and Z. Šipuš, Active wireless sensor with radio frequency identification chip, IEEE Proceedings of the 35th International Convention MIPRO, pp.727–732, 2012.

[61] J. Tan and S. G. M. Koo A survey of technologies in internet of things, IEEE International Conference on Distributed Computing in Sensor Systems, pp.269–274, 2014.

[62] B. Nath, F. Reynolds and R. Want, RFID technology and applications, IEEE Pervasive computing, Vol5, No.1, pp.22-24, 2006).

[63] R. Want, An introduction to RFID technology, IEEE pervasive computing, Vol.5, No.1, pp.25-33, 2006.

[64] R. Want, Near field communication, IEEE Pervasive Computing, Vol.10, No.3 pp.4-7, 2011.

[65] M. Jia, A. Komeily, Y. Wang and R. S. Srinivasan, Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applicationsm, Automation in Construction, Vol.101, pp.111-126, 2019.

[66] IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE 802 Working Group, IEEE Std. 802.15.4, 2011.

[67] J. Song, et al. WirelessHART: Applying wireless technology in real-time industrial process control, IEEE Real-Time and Embedded Technology and Applications Symposium, pp.377-386, 2008.

[68] R. Frank, W. Bronzi, G. Castignani and T. Engel, Bluetooth low energy: An alternative technology for VANET applications, IEEE 11th annual conference on wireless on-demand network systems and services (WONS), pp.104-107, 2014.

[69] J. DeCuir, Introducing bluetooth smart: Part 1: A look at both classic and new technologies. IEEE Consumer Electronics Magazine, Vol.3, No.1, pp.12-18, 2013.

[70] E. Mackensen, M. Lai and T. M. Wendt Bluetooth Low Energy (BLE) based wireless sensors. Sensors, IEEE, pp.1-4, 2012.

[71] M. Siekkinen, M. Hiienkari, J. K. Nurminen and J. Nieminen, How low energy is bluetooth low

energy? comparative measurements with zigbee/802.15.4, IEEE wireless communications and networking conference workshops (WCNCW), pp.232-237, 2012.
[72] M. Jung, et al. A transparent ipv6 multi-protocol gateway to integrate building automation systems in the internet of things, IEEE International Conference on Green Computing and Communications, pp.225-233, 2012.
[73] C. Hennebert and J. Dos Santos, Security protocols and privacy issues into 6LoWPAN stack: A synthesism IEEE Internet of Things Journal, Vol.1, No.5, pp.384-398, 2014.
[74] M. R. Abdmeziem, D. Tandjaoui and I. Romdhani, Architecting the internet of things: state of the art, Robots and Sensor Clouds, pp.55-75, 2016.
[75] Jie. Lin, et al. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet of Things Journal, Vol.4, No.5, pp. 1125-1142 2017.
[76] C. Bormann, A. P. Castellani and Z. Shelby Coap: An application protocol for billions of tiny internet nodes, IEEE Internet Computing, Vol.16, No.2, pp.62-67, 2012).
[77] W. Gao, J. Nguyen, W. Yu, C. Lu and D. Ku, Assessing performance of constrained application protocol (CoAP) in MANET using emulation, Proceedings of the International Conference on Research in Adaptive and Convergent Systems, pp.103–108, 2016.
[78] U. Hunkeler, H. L. Truong and A. Stanford-Clark, MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks, IEEE 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08), pp.791–798, 2008.
[79] X. Xu, D. Yuan and J. Wan An enhanced routing protocol for ZigBee/IEEE 802.15. 4 wireless networksc IEEE Second International Conference on Future Generation Communication and Networking, Vol.1, 2008.
[80] P. Baronti, et al. Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards, Computer communications, Vol.30, No.7, pp.1655-1695, 2007.
[81] P. Spachos, I. Papapanagiotou and K. N. Plataniotis, Microlocation for smart buildings in the era of the internet of things: A survey of technologies, techniques, and approaches, IEEE Signal Processing Magazine, Vol.35. No.5, pp.140-152, 2018,.
[82] H. B. Pandya and T. A. Champaneria, Notice of Removal: Internet of things: Survey and case studies, IEEE international conference on electrical, electronics, signals, communication and optimization (EESCO), pp.1–6, 2015.
[83] C. Gomez and J. Paradells Wireless home automation networks: A survey of architectures and technologies, IEEE Communications Magazine, Vol.48, No.6, pp.92-101, 2010.
[84] A. B. Forouzan, Data communications & networking (sie), Tata McGraw-Hill Education, 2007.
[85] B. Meador, A survey of computer network topology and analysis examples, Washington University, pp.2-3, 2008.
[86] D. A. Gratton, The handbook of personal area networking technologies and protocols, Cambridge University Press, 2013.
[87] L. Schor, P. Sommer and R. Wattenhofer Towards a zero-configuration wireless sensor network architecture for smart buildings, Proceedings of the First ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings, pp.31–36, 2009.
[88] J. Pan, et al. An internet of things framework for smart energy in buildings: designs, prototype, and experiments, IEEE Internet of Things Journal, Vol.2, No.6, pp. 527-537, 2015.
[89] D. Balsamo, G. Gallo, D. Brunelli and L. Benini, Non-intrusive zigbee power meter for load monitoring in smart buildings, IEEE Sensors Applications Symposium (SAS), pp.1-6, 2015.
[90] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang and P. P. Gupta, Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings, Future Generation Computer Systems, Vol.82, pp. 349-357, 2018.
[91] A. J. Snyders, H. C. Ferreira and P. J. V. Rensburg, Modeling of coupling diversity for Extra-Low-Voltage power-line communication networked LED lighting in smart buildings, IEEE Journal of Emerging and Selected Topics in Power Electronics, Vol.6, No.3, pp. 1224-1234, 2018.
[92] D. Li, Z. Kun and Q. Gao, Zero energy consumption LED intelligent lighting system based on the technology of PoE. 37th Chinese Control Conference (CCC), pp.7639–7643, 2018.
[93] J. F. Schmidt, D. Chernov, M. Pauritsch and C. Bettstetter Study of a self-powered UWB sensor network for industrial applications, European Wireless 2019; 25th European Wireless Conference, VDE, pp.1-6, 2019.
[94] A. Corna, L. Fontana, A. A. Nacci and D. Sciuto, Occupancy detection via iBeacon on Android devices for smart building management, Design, Automation and Test in Europe Conference and Exhibition (DATE), pp.629–632, 2015.
[95] S. Alletto, et al. An indoor location-aware system for an IoT-based smart museum, IEEE Internet of Things Journal, Vol.3, No.2, pp.244-253, 2015.
[96] V. Moreno, M. A. Zamora and A. F. Skarmeta, A low-cost indoor localization system for energy sustainability in smart buildings, IEEE sensors journal, Vol.16, No.9, pp.3246-3262, 2016.
[97] S. D. Tebje Kelly, N. K. Suryadevara and S. C. Mukhopadhyay, Towards the implementation of IoT for environmental condition monitoring

in homes, IEEE sensors journal, Vol.13, No.10, pp. 3846-3853, 2013.

[98] C. Peng, K. Qian and C. Wang. Design and application of a VOC-monitoring system based on a ZigBee wireless sensor network, IEEE Sensors Journal, Vol.15, No.4, pp. 2255-2268, 2014.

[99] R. K. Kodali and B. S. Sarjerao MQTT based air quality monitoring, IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017.

[100] A. A. Hapsari, et al. Real time Indoor Air Quality monitoring system based on IoT using MQTT and wireless sensor network, IEEE 6th International Conference on Engineering Technologies and Applied Sciences (ICETAS), pp.1-7, 2019.

[101] P. Oksa, M. Soini, L. Sydänheimo and M. Kivikoski, Kilavi platform for wireless building automation Energy and Buildings, Vol.40, No.9, pp.1721-1730, 2008.

[102] Z. Shelby, Embedded web services, IEEE Wireless Communications, Vol.17. No.6, pp.52-57, 2010.

[103] K. Khanchuea, R. Siripokarpirom, A multi-protocol IoT gateway and WiFi/BLE sensor nodes for smart home and building automation: Design and Implementation. IEEE 10th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES), pp.1-6, 2019.

[104] P. Morgner, S. Mattejat and Z. Benenson, All your bulbs are belong to us: Investigating the current state of security in connected lighting systems, arXiv preprint arXiv:1608.03732, 2016.

[105] I. Unwala, Z. Taqvi and J. Lu, IoT security: ZWave and thread, IEEE Green Technologies Conference (GreenTech), pp.176–182, 2018.

[106] K. S. Aloufi and O. H. Alhazm, Performance analysis of the hybrid iot security model of mqtt and uma, arXiv preprint arXiv:2005.06595, 2020.