UNIVERSITY OF ALBERTA

MINT 709

Project Report on

Design and requirements of IoT based smart buildings

Submitted By:

Priya Saini

In partial fulfillment for the award of the degree

Master of Science in Internetworking

(From University of Alberta)

Under the guidance of

Juned Noonari

Acknowledgment

I would like to express my heartfelt gratitude to my family for supporting my study towards the Master of Science in Internetworking at the University of Alberta.

Also, I would like to thank Juned Noonari, for his mentorship and untiring commitment in guiding and encouraging me to understand and overcome problems that would otherwise have stopped me midway. In addition to this, I appreciate him for being always approachable and guiding me with frequent comments and suggestions about the project.

I would also take this opportunity to thank Dr. Mike MacGregor for approving the project so that I can work on it.

Last but not least, I would like to thank all unnamed people who have willingly helped me out with their abilities.

Abstract

In recent years, the popularity of IoT based smart building technology has been rising at an unprecedented rate. It is estimated that the IoT based smart buildings market will grow over USD 31 billion by the year 2022 [42]. IoT devices are building blocks of smart buildings, hence it is essential to know about the applications, benefits, advantages, and disadvantages before designing or implementing a layout to determine the best-case scenario as it is a very broad technology.

This report focuses on a thorough explanation of IoT, its importance while explaining its history and background. It talks about the evolution of IoT in many sectors resulting in ease of access and advancement in technology. IoT protocols and architecture are also explained to give a better picture to deploy it. Furthermore, it reveals facts regarding smart buildings and the way they work to control the building environment automatically.

In addition to that, this project talks about the evolution of the IoT based smart buildings, its transition, and technologies used for making them intelligent. It shows non-energy benefits for the business owners to flourish in the market while adapting to this advancement. In addition, this project also talks about smart building examples to explain its features.

This report further dives into the discussion of the security aspect of smart buildings describing the challenges during the whole journey of converting any infrastructure into a smart building with potential security solutions to overcome them. Also, it briefly explains the advantages and disadvantages in the field of smart buildings. Moreover, the future scope of these smart buildings shows its future growth in the market.

Finally, towards the end, it focuses on the real-life case study to explain IoT based smart building projects where a significant reduction in the cost of building maintenance and energy consumption was achieved, maintaining a more comfortable living environment at the same time.

Table of Contents

1 Introduction 6

1.1 What is the Internet of Things? 6

1.2 History and Background 9

1.3 How does the IoT system work? 11

1.3.1 Examples of IoT 13

1.4 Evolution in various sectors 15

1.5 IoT reference architecture 23

1.5.1 IoT reference architecture requirements 24

1.5.2 The Architecture 29

1.6 IoT protocols 39

1.6.1 Network protocols 39

1.6.2 Data protocols 46

1.7 IoT conclusion 50

1.8 What is a smart building? 50

1.9 History and Evolution 61

1.10 How does a smart building system work? 63

1.11 What can a smart building do? 64

1.12 SB conclusion 65

2 Correlation between IoT and smart buildings 67

2.1 Difference between IoT Smart Buildings with and without integration 73

2.1.1 Smart Building with integration 73

2.1.2 Smart Building without integration 74

2.2 Components of smart buildings 75

2.3 What makes smart buildings "smart"? 78

2.4 Non-energy benefits of smart building 81

2.5 Existing smart building technologies 82

2.5.1 Examples of smart buildings 90

3 Security issues and challenges for the IoT based smart building 99
3.1 Security issues in smart building 99
3.2 Challenges for smart buildings 104
3.3 Security solutions for smart buildings 105
3.4 Pros and Cons of IoT based smart buildings 111
3.4.1 Advantages 111
3.4.2 Disadvantages 114
3.5 The future scope of IoT based smart building 116
4 Case Study: Design and Technologies for implementing a smart educational building 121
5 Conclusion 127
Appendix A: List of Figures 129
Appendix B: Reference 131

1 Introduction

The Internet of Things based Smart Building is the smart application of digital technology to solve the automation requirements of an analog world. There are two crucial fundamentals to IoT based Smart Building: Digital automation and the Internet itself. This section contains a comprehensive introduction to the Internet of Things (IoT), it will also give extensive information regarding Smart Buildings and some other important points that will be discussed as well.

1.1 What is the Internet of Things?

The Internet of Things (IoT) reflects the technological revolution that represents the future of computing and communications. The advancement in the area of the Internet of Things (IoT) has seen in the past two decades. It has attracted numerous researchers and industries because of its significant effect on our daily life. The term “Internet of Things,” which is also known as IoT, is made up of two words, such as the first word is “Internet,” and the second words are “Things.” The Internet is a global system of computer networks connected to one another. Where TCP/IP (Transmission Control Protocol/Internet Protocol) is used to interchange the information between computers and computer networks and telecommunication networks are utilized to connect the computers. Communication has become much more comfortable than before the internet. As the internet could be used for email, transfer files, and obtain the information on the worldwide web.

On the other hand, Things are real objects in this physical and material world. It can be any object or person which could be recognized separately in the world. It means here things can be both living things like a human being, plants- coconut tree, mango tree and cacao tree, animals- dog, rabbit and dolphins, and many more. Furthermore, non-living things like electronic devices we encounter and use daily such as a chair, desk, and so many [1].

Besides, there are many definitions available for the Internet of things, depending on who is defining it. However, the basic concept of the Internet of Things (IoT) is where all the physical devices (things) around the world connect through the internet. Such devices are smartphones, sensors, wearables, and many more that can share information over the internet without requiring human to human or human to computer interaction.

There are four critical elements in IoT:

1. People use internet-connected end-nodes to share data and activities, including social networks, health sensors, and fitness sensors [3].

2. Devices, physical sensors, actuators, and other items that create or receive data from other sources to communicate. For instance, smart thermostats and devices for smart homes [3].

3. Raw data is processed and turned into useful information to create smart decision-making and control mechanisms [3].

4. The process of taking advantage of connectivity is to add value between data, things, and people. For example, smart fitness equipment, such as fitness watches, can be used to advertise healthcare services to prospective customers [3].

Therefore, the Internet of Things is a crucial process for automation, where data is the heart of the Internet of Things and is gathered, analyzed, and reacted accordingly. Many technologies are combined by the Internet of Things to create new revenue streams as well as new values.

The Internet of Things is beneficial for many applications and services in the real world, as well as applicable to build a smart home or smart buildings. For example, When the air conditioner is turned on, the windows can be automatically closed or opened to oxygen when the gas oven is turned on.

Figure 1. The Internet of Things.

Source: https://s22908.pcdn.co/wp-content/uploads/2017/01/what-is-internet-of-things.jpg

Moreover, the concept of IoT is particularly valuable for people with disabilities, as IoT systems can help larger-scale human activities such as building or society, as the devices can collaborate to function as a whole system.

There are two essential features of IoT:

The devices, as well as the server-side architecture that helps them. Often, there is a third category, as well. Whereas, in most of the cases, there may be a low-power gateway that conducts event processing, bridging, and aggregation. Perhaps that lies between devices and the internet [9].

However, in both cases, there is probably an intermittent connection in the devices based on their factors like battery discharging, radio interference, GPRS connectivity, and many more [9].

There are different classes of IoT devices which are explained below as well as in figure:

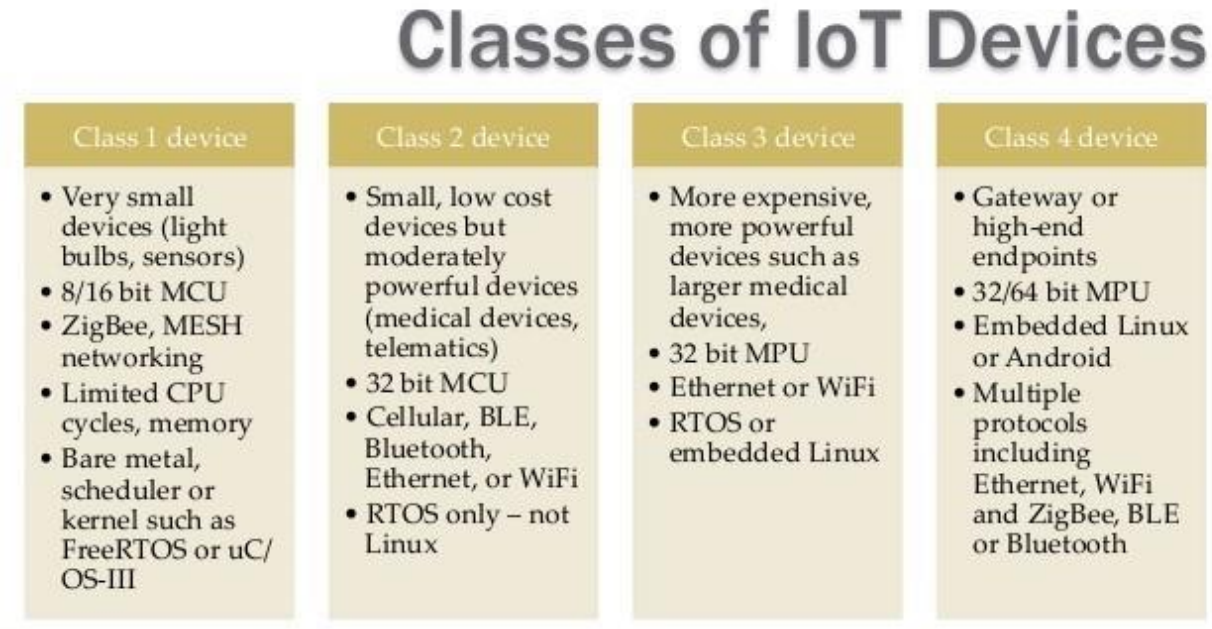


Figure 2. Classes of IoT devices.

Source: https://image.slidesharecdn.com/2015-09-16aimee-150924123805-lva1-app6892/95/security-fundamental-for-iot-devices-creating-the-internet-of-secure-things-15-638.jpg?cb=1443098338

1. 8-bit System-On-Chip (SOC) controllers are embedded in the smallest devices. An excellent example of this would be an open-source hardware platform, Arduino. For example, the Arduino Uno platform and another 8-bit Arduinos. Mostly, they do not have an operating system [9].

2. Atheros and ARM chips, which have a minimal 32-bit architecture, are the next level up. Frequently, these add small house routers and derivatives of those devices. It is an embedded Linux platform such as OpenWRT. Sometimes they might not use the operating system, for example, Arduino Zero [9].

3. The most competent IoT platforms are complete 32-bit or 64-bit computing platforms. The Raspberry pi and the Beadglebone are the systems that might run a full Linux operating system or another kind of operating system like Android most of the time; these are whether mobile phone or the mobile phone technology [9].

For smaller devices, these devices act as gateways or bridges. For instance, when a watch (wearable) is connected through Bluetooth to a mobile phone that bridges that onto the more large-scale internet [9]. Moreover, there are many different models to the communication between devices and the internet or to a gateway, which includes Wireless connection using TCP or UDP, Direct Ethernet, Bluetooth, Near Field Communication (NFC), Zigbee, point to point links and many more [9].

1.2 History and Background

The Internet of things was not around for a long time as the concept officially named until 1999. The first example of the Internet of Things was a Coca Cola machine located at the Carnegie Mellon University in early1980. Where local programmers will connect to the refrigerated device through the Internet to search to see if a drink was available and if it was cold before making the trip [5].

The first to describe the Internet of Things was Kevin Ashton, the Executive of Auto-ID Labs at MIT in 1999, while making a presentation for Procter and Gamble. During the speech, Mr. Ashton Stated: "Today computers and the Internet rely almost entirely on people for knowledge. Nearly 50 petabytes (a petabyte per 1024 terabytes) of data available on the Internet.

It was first captured and generated by humans by typing, clicking a record button, taking a digital image, or scanning a barcode. The problem is that people have a limited amount of time, care, and precision. All that means they are not very good at capturing real-world data about things.

He also explained that if we had computers, it would reduce waste, loss, and cost as everything would be able to track and count. Computers would know everything about things, and they would gather data without any help from humans or, in simple words, they could perform independently [5].

Connecting the devices in new ways

The idea of IoT is any device capable of interconnecting with other devices. IoT technologies are finding new ideas in many ways, which will contribute to the activities already in use. For example, let's assume an alarm is waking you up at 6 AM and then signaling the coffee maker to turn on and start brewing coffee at the same moment. Also, let assume the printer knows when we are out of paper or running low, and it will automatically do the ordering. The IoT based smartwatch will tell us when we were most productive. Moreover, the Internet of Things can be used to organize things like transportation networks. "Smart Cities" can use this to reduce waste and improve energy efficiency [5].

To interconnect devices and equipment, IoT provides an approximately endless supply of opportunities. And, the Internet of things provides opportunities as well as potential security problems [5].

In addition, the Internet of things has been around for over a decade; two technologies have been very crucial behind the rise of IoT in the last twenty years. The first one is tremendous growth in mobile devices and various applications, and the second one is the high availability of wireless connectivity [6].

According to the 2011 report from Cisco, approximately 500 million devices connected to the Internet in 2003, most probably all the personal computers. And if we divide the number of connected devices by the world population, which was at 6.3 billion. That time there was less than one (0.08) device available for every person on the planet. However, by 2010, there was a dramatic rise in the smartphone and tablet market as the number of connected devices increased up to 12.5

billion. Yet, the world's population grew to just 6.8 billion. Therefore, in only seven years, the rate of connected devices rose from 0.08 to 1.8. It means the connected devices per person in the world increased by 2,250 percent [6].

Furthermore, other development was way beyond than mobile technology which was sensors. It had a higher cost in the 20th century that resulted in the limited use of sensors. For instance, solid-state image sensors cost 20 dollars to 25 dollars, but by the end of the decade, it was sold for 5 dollars. which leads to a massive increase in the digital camera market. In fact, other sensors like the one found in smartphones were also very costly; for example, the accelerometers sensor used for adjusting an orientation of the app screen in the smartphones cost around 7 dollars in 2007. however, presently it costs less than 0.50 dollars [6].

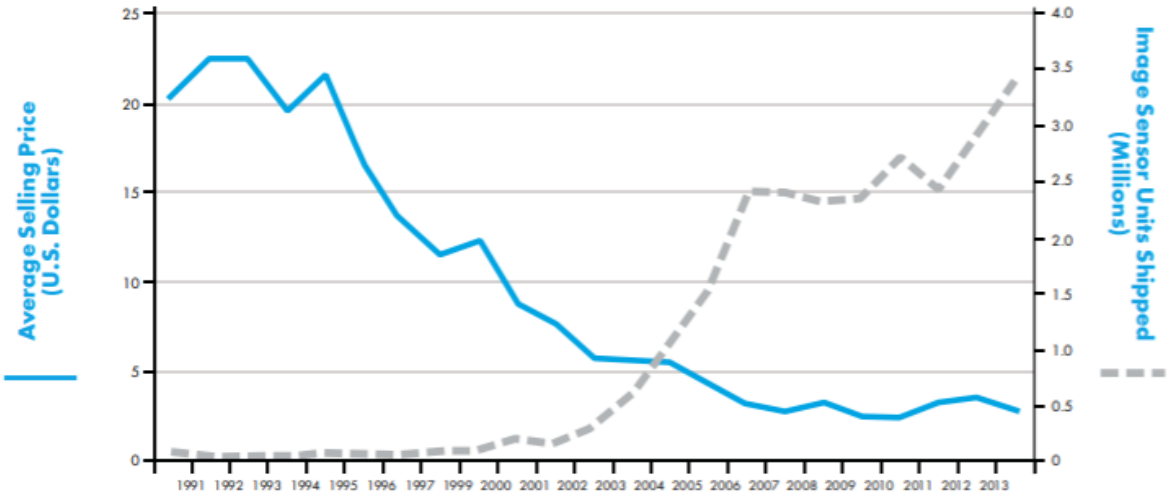


Figure 3. Flow chart

Source: https://www.aig.com/content/dam/aig/america-canada/us/documents/insights/aig-white-paper-iot-english-digital-brochure.pdf

1.3 How does the IoT system work?

A whole IoT system combines four different elements, such as sensors or devices, connectivity, data processing, and a user interface. All these elements work simultaneously to achieve automation; these are explained briefly in the following sections.

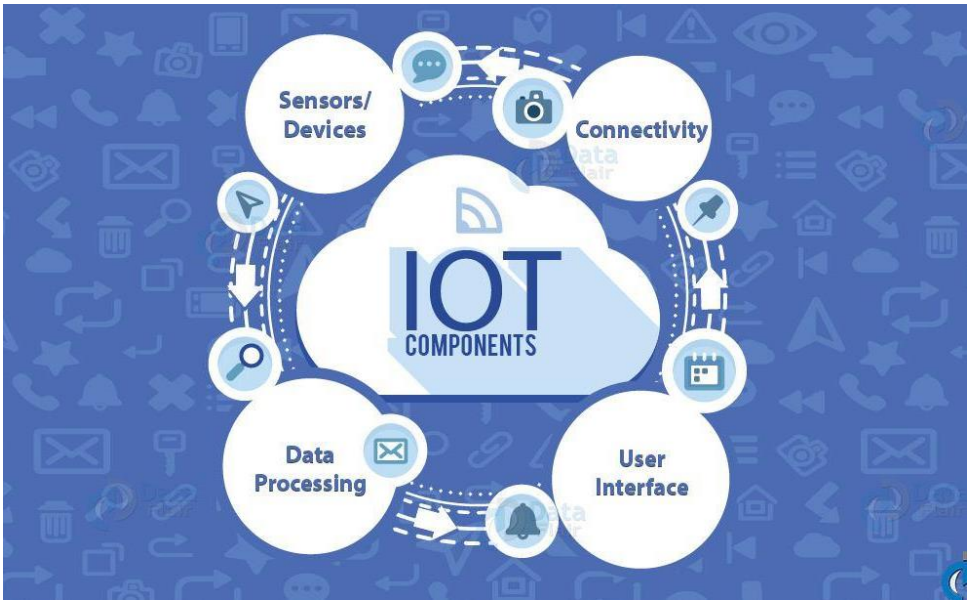


Figure 4. How does the IoT system work?

Source: https://d2h0cx97tjks2p.cloudfront.net/blogs/wp-content/uploads/sites/2/2018/05/IOT-Components.jpg

1. Sensors or Devices:

Firstly, with the use of sensors or devices, the data is gathered from the environment. For example, a simple task as a temperature reading or a complex task as full video feed (skype). Sensors or devices, for instance, phone, camera, accelerometer, and GPS [4].

2. Connectivity:

Secondly, various methods are utilized, such as cellular, Bluetooth, satellite, WiFi, ethernet, and many more, to send the data to the cloud. In other words, sensors or devices are connected to one of these methods and then send the data to the cloud [4].

3. Data Processing:

Thirdly**,** when the data reaches the cloud, then software conducts some processing on it. It can be a simple task like checking that the reading of the temperature is within an acceptable range, or it might also be a very complicated task to identify objects (such as intruders in your home) by using computer vision on video [4].

4. User Interface:

At last, the detail is in some way made accessible to the end-user. It could be done through a user alert like email, message, and notification. For instance, a text alert if the temperature in the company's cold storage is too high. Or if there is an intruder inside the house.

Furthermore, the system can be checked proactively through an interface that may be handled by a user. For example, a user can check the video feed of their house via a phone or web browser. And, they can perform some actions accordingly like remotely modify the temperature in the cold storage through a phone on their own. Or some actions can be done automatically via predefined rules rather than waiting for an external help [4]

1.3.1 Examples of IoT

In these examples, it will explain how IoT works in real life:

I. Scenario: AC temperature sensors

1. In our room, we have an AC (Air conditioner) in which the temperature sensor was installed. The room will integrate with a gateway, and the purpose of the gateway is to connect the temperature sensor that is inside the AC to the Internet using cloud or server infrastructure [4].
2. The details regarding every device connected to the AC like device status, device id, how many devices connect to it, what was the last time the device accessed, and by whom and how many times the device has approached are recorded by the cloud or server infrastructure [4].
3. Then, a connection to the cloud will be implemented by using web services, namely RESTful [4].
4. In this step, end-users interact with the cloud (and it connects to the devices installed at our house) using a mobile application. Therefore, a request would submit the user and device information to the cloud infrastructure with authentication. To maintain cybersecurity, it needs system authentication [4].
5. When the cloud has authenticated the device A request is sent through the gateway to the appropriate sensor networks [4].

6. After getting the request, the temperature sensor inside the AC will read the recent temperature and submit the response back to the cloud [4].
7. At last, the cloud infrastructure will distinguish the specific person or user who has requested the data and transfer the required data to the mobile application. On the other hand, a user will receive information regarding the current temperature in the room, which is accessible by the AC's temperature sensors on his mobile application [4].

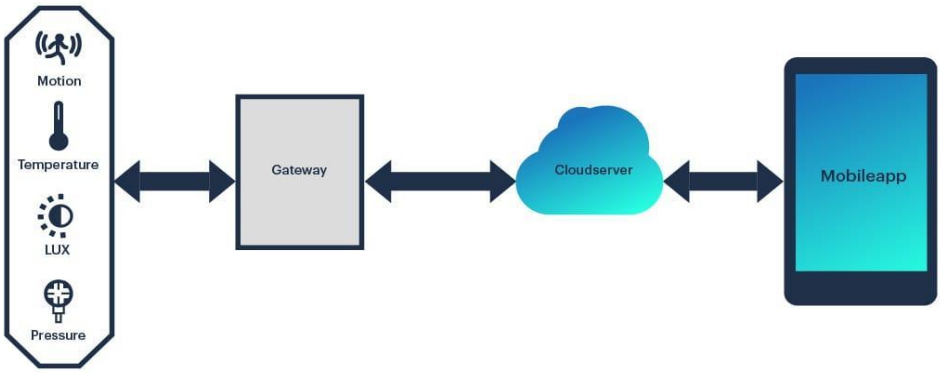


Figure 5. AC temperature sensor

Source: https://www.baianat.com/articles/how-iot-is-transforming-industries

II. Scenario: IoT in Home

Imagine waking up Angel at 6 am every day for work, the alarm clock will do the work for just waking up. Until due to some reasons, something goes wrong such as the train got canceled. That time, Angel must drive to work instead of taking the Bus. Here the problem is, Angel must wake up early at 5.45 am to reach work on time. Moreover, it is raining outside, so Angel must drive slower than usual.

In these factors, an IoT based alarm clock or a connected alarm clock to the internet will reset itself based on all as well as it will ensure that Angel reaches at work on time.

The IoT based Alarm clock recognized that the train had been canceled, and it will check the weather. It will automatically calculate the driving distance and travel time (because of heavy rain) to reach work on time.

It will also calculate when it is needed to wake up so that Angel will not be late for work. IoT based alarm clocks can be smarter if they are synchronized with IoT based coffee makers to assure the morning coffee is ready to go.

Alternatively, in other cases like daylight saving, an IoT based alarm clock will change its time accordingly.

1.4 Evolution in various sectors

In this era, most of the companies have adopted the Internet of Things. To be sure, in the coming years, there would be no industry that is not connected to the IoT. While using the Internet of Things, many Industries have improved their long-term strategies to increase profit. Here, some examples have been utilized to explain how specific companies and sectors have begun using IoT, which are as following:

1) Automobile:

Because of motor vehicle accidents, 1.24 million people died worldwide every year on average, according to the report of the World Health Organization. In Europe every year, the cause of the death of approximately 30,000 people was a motor vehicle accident. Even it is the same in the USA. However, this issue is far worse in Asia as only in China and India every year, approximately 400,000 people die in a motor vehicle accident [6].

With the time these automobile companies have started to adopt IoT technologies, especially to increase safety-focused sensors on automobiles, as a promise to reduce motor vehicle accidents as well as to reduce the global death rate [6].

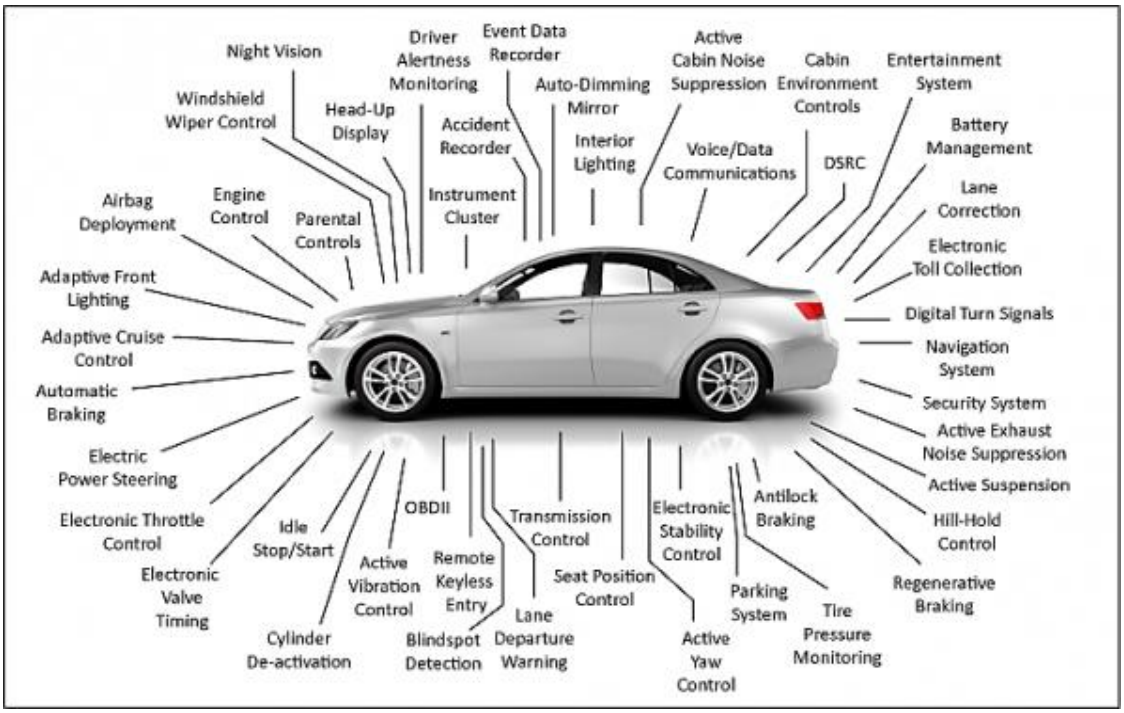


Figure 6. Automobiles advancements.

Source: https://www.eenewseurope.com/design-center/automotive-service-era-electronic-car-1

In May 2015, there was an announcement by the German-Owned, U.S.-based Daimler Trucks North America company that they were ready to testify their driverless Freightliner Inspiration Truck on Nevada roadways. Although Google and Tesla are also developing their driverless cars, which are slowly coming online, some safety sensors give a 360-degree view of the vehicle, and some of the safety sensors work autonomously to protect the vehicle without driver action directly [6].

As most of the accidents are done because of human error and to reduce the accidents, the rational decision-making component in driving will be changed to autonomous vehicles. Moreover, the data is also collected by the automobile companies to produce more efficient cars, yet there are some security concerns regarding the data collection, which will explain later [6].

2) Infrastructure:

The Internet of Things technology has used in many industries and companies to improve efficiency and safety. This technology is beneficial to diminish the various risks inside or outside

the sectors. Whereas, many hazards like floods, fires, and others, affect the business in some way. However, the Internet of Things, especially embedded sensors, can remove the risk in some specific areas [6].

For instance, the electrical system can be monitored by using sensors that will detect the flow of electricity through a building. When something went wrong, connection failed or about to fail, the possibility of fire or any other crisis. These sensors will instantly warn the technicians, or it will give an emergency alert to resolve the problem [6].

The IoT based sensors are also used in the data center. It helps to maintain cooling inside the data center, and if the temperature starts to rise, it will give an alert to employees. These sensors also detect if any Heat Ventilation Air Conditioner or boiler malfunction occurs. Moreover, the data is captured by these embedded sensors to analyze and identify the hints for resolving future issues [6].

On the other hand, the utilization of energy in the industry efficiently can also be balanced by IoT technology. For example, an office building with multiple levels can monitor the energy consumption form each floor, and the data will be captured and analyzed to check whether the energy is getting waste or where to cut the cost to make the industry more efficient [6].

3) Banking sector:

The Internet of Things technology focuses on making the financial sector or banking sector more efficient. The first step was to achieve it using mobile technology for mobile banking, which has made the tasks easier for the customers.

For instance, by using IoT sensing technology for the banking ATM, one day, a user with the correct biometric identification might withdraw the cash from the ATM without using his debit card [6].

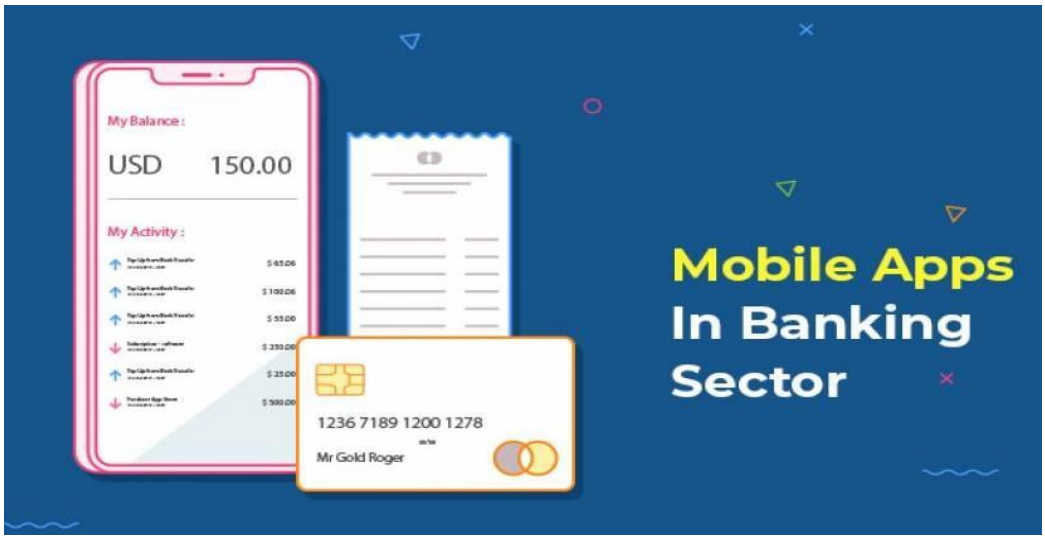


Figure 7. Banking sector (Mobile banking)

Another example is, the financial portfolio would be connected to the user's health monitor so that at the time of crisis, which would be captured by the monitor can notify the user's back for automatically rebalancing his portfolio to drop his financial exposure [6].

4) Aerospace sector:

Aerospace technology has evolved, which can be seen from the last decades. It was possible because of the Internet of Things. The system named "Fly-by-wire" is a mainstay of the aerospace sector, which is based on the Internet of things [6].

Due to this system, the conventional manual flight control of an airplane has been replaced with an electronic interface where the pilot focuses on monitoring the plane only [6]. At the same time, the sensors and the automation systems handle everything of the rest [7].

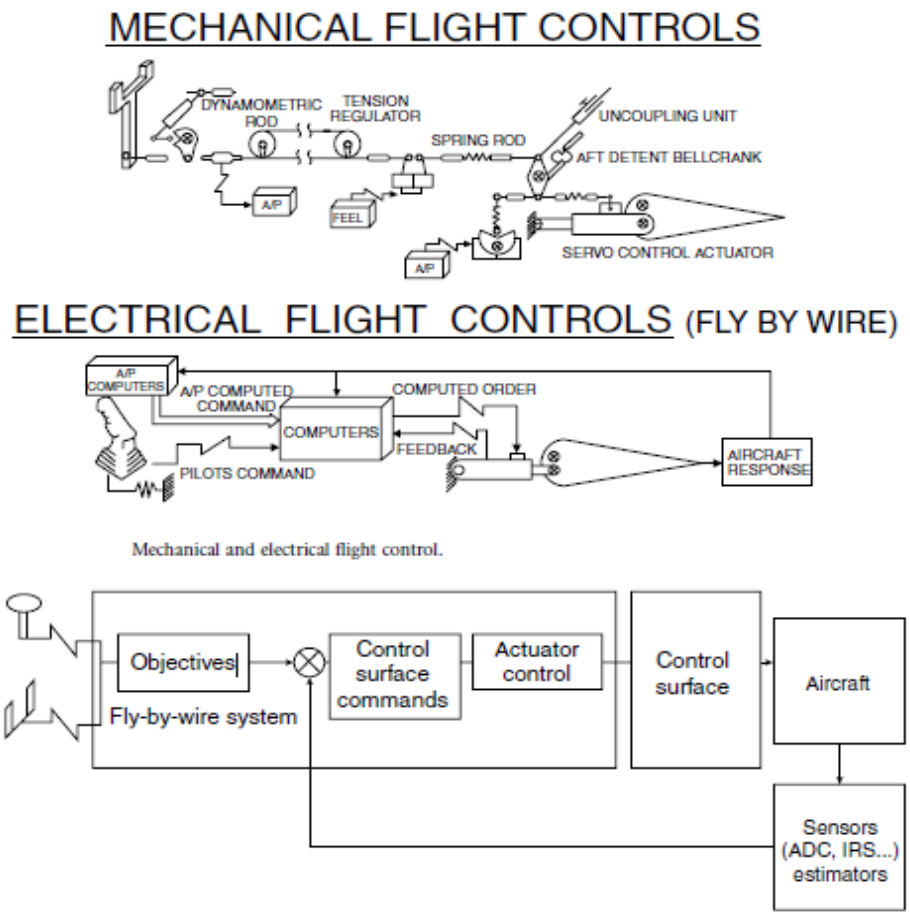


Figure 8. Fly-by-wire

Source: https://fcs4987.wordpress.com/2013/12/08/flight-controls-and-fly-by-wire/

The "Fly-By-Wire" system has become so advanced in many ways that airplane vehicles are virtually autonomous. It saves planes from accidents or in other emergencies, and there is a real example available to justify it. In 2009, Captain Chesley B. "Sully" Sullenberger was able to make an emergency landing in the Hudson River after taking off from New York's LaGuardia Airport. Captain Chesley B. "Sully" Sullenberger was flying the Airbus A320, which first introduced the use of automated "Fly-By-Wire" systems. The highly advanced sensors saved the plane from crashing while rescuing all the 155 people aboard and the incident known as the "Miracle on the Hudson" [6].

IoT technology does not only provide safety but also provides efficiency to the aerospace sector. On the ground level, the Internet of Things technology is being used by aerospace companies to improve the maintenance and safety arrangements. For instance, the aircraft engine maintenance companies are using onboard sensors in airplane engines to collect real-time information regarding engine performance. Also, the data produced by this process would be analyzed to increase engine efficiency, reduce fuel costs, and decrease travel time [6].

In figure 1.1.2.1(4), it briefly explains a digital Fly-By-Wire control system complex software compiles signals from the pilot's control input sensors and then executes some computation on the data generated by the sensors, to achieve the desired path [7].

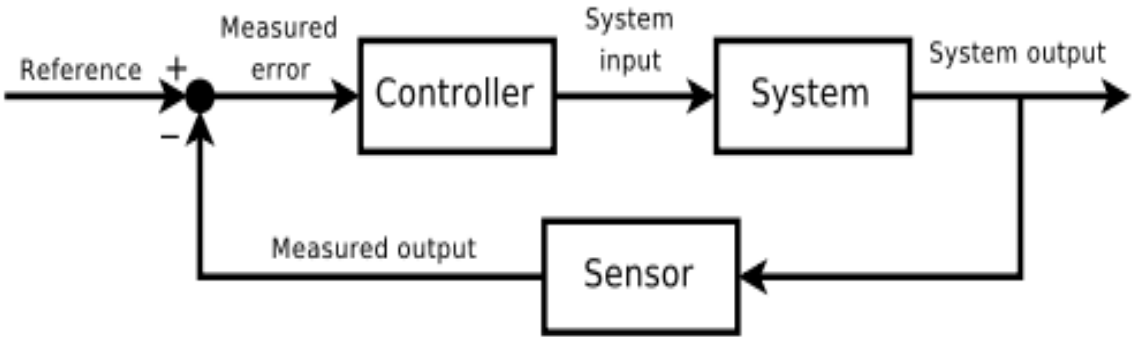


Figure 9. Explain how the Fly-By-Wire system works

Source: https://fcs4987.wordpress.com/2013/12/08/flight-controls-and-fly-by-wire/

5) Healthcare department:

The Internet of things or the Internet of Medical Things (IoMT) is described as a collection of the medical equipment and applications which are connected to the IT sector in Healthcare via online computer networks [8].

In 2016, as per a report generated by the National Institutes of Health, 8.5 % of the world's population was older, and this ratio is increasing drastically day by day. Moreover, this is estimated to reach approximately 17% by 2050. Society's expectation has also risen for more and better health services and to provide healthcare and hospital facilities; there is a need to push the current systems beyond its limits [8] and explain in the figure.

Figure 10. Healthcare IoT

Source: https://www.ubuntupit.com/iot-in-healthcare-20-examples-thatll-make-you-feel-better/

Fortunately, IoT technology has integrated into the healthcare sector to create advanced medical applications. Whereas, wireless technology has been practiced in the healthcare sector for many years; however, it is rapidly associating into the healthcare department, enhancing the healthcare services more and more. Due to healthcare IoT, doctors can effectively diagnose and treat patients, manage prescriptions while prescribing targeted and better medications to avoid allergy because of medicine, as well as enhance hospital staff coordination and efficiency [8].

Healthcare departments are adopting IoT technology in many ways to provide better facilities for people that are explained in the following sections [8]:

1. Many devices are interconnected with each other, and they are continuously generating the data. This big data can be stored in the healthcare data center, or it can be moved to the cloud. And at a certain point, IoT will be the most significant source of data. Furthermore, this data will be used by healthcare practitioners to learn and make better decisions and predict current and later health issues [8]. Due to this, it makes it easy to get the correct information regarding a patient as well as it is also very time-saving. Show in the figure as well:

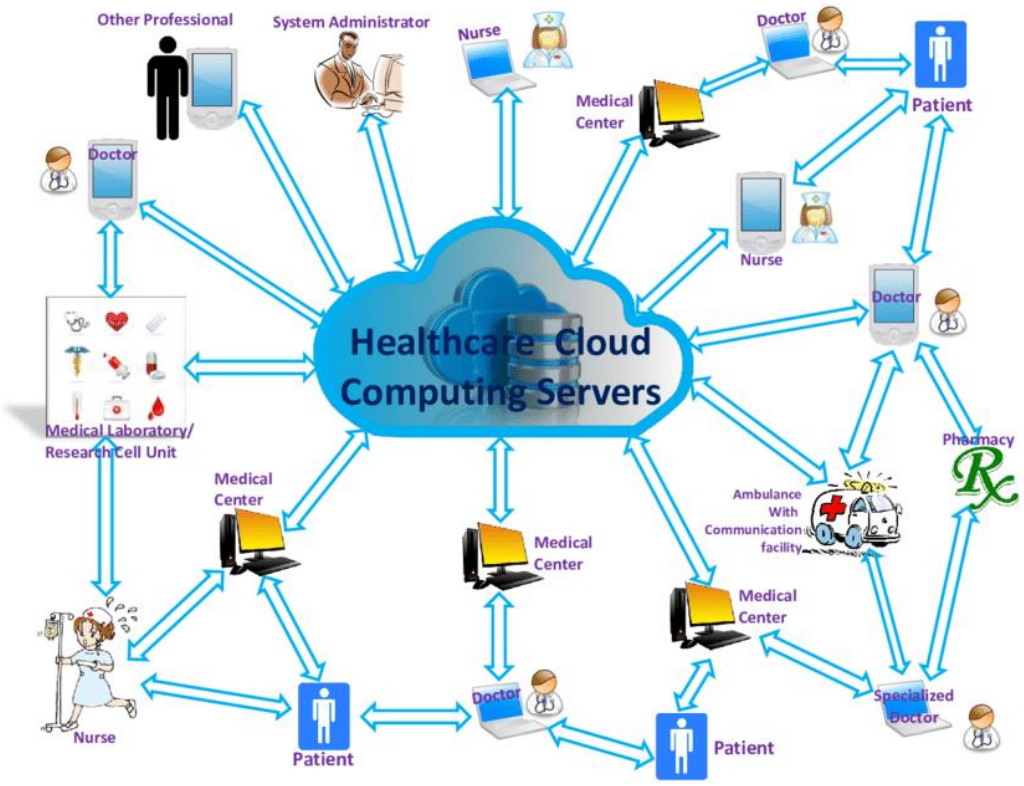


Figure 11. Cloud in the healthcare sector

Source: https://www.researchgate.net/figure/High-level-illustration-of-healthcare-cloud_fig6_320093536

2. Nowadays, medical drones are used for rescue purposes. It is beneficial, especially for the rural areas where it is hard to reach by the medical. Recently, the "Flying IoT" drones are used to transport medical supplies such as red blood cells, platelets, and plasma in a life-threatening case in Rwanda. Moreover, in these days, drones are used for many activities like delivering medical supplies to save time [8].

   Many companies are testing IoT drones as medical delivery transportation and they are also accepting it, and it is just a question of time that this technology (IoT drones) will be adopted universally for the healthcare sector [8]. Shown in the figure as well:

Figure 12. IoT drone

Source: https://www.healthcarepackaging.com/markets/medical-device-packaginig/news/13702056/montreal-is-testing-drones-as-medical-delivery-vehicles

Although there are some IoT concerns or IoT security problems which will be discussed later, still IoT provides many benefits in many areas, which makes human life easier.

1.5 IoT reference architecture

The Internet of Things is everywhere, the connection among people and things is increasing in large numbers, and the data is generating on a large scale, which was unimaginable once [10]. Therefore, architecture is an ideal framework to understand relationships among the objects of any environment [10]. Furthermore, the Internet of Things architecture allows us to get a deep understanding of the IoT system.

Also, a different communication and processing model requires the network, data management, and application design. Although still, there is no standard way available for defining these IoT models, which result in confusion between IoT or non-IoT devices and systems, So, there is a need for a good IoT reference architecture [10].

There are many reasons why a reference architecture for IoT a good thing is and why it is needed, which are as follow:

- The IoT reference architecture makes everything simple by breaking down the complicated systems to make each component easier to understand [10].
- It clarifies things by providing extra information to identify IoT levels accurately as well as to build a standard terminology [10].
- It defines where different types of processing optimize throughout numerous parts of the system [10].
- It standardizes the Internet of Things by allowing the vendors to create IoT products that can work with each other [10].
- It makes the IoT more convenient and real, rather than merely conceptual [10].
- Moreover, IoT devices are closely connected, and a way is needed to interact with them regardless of the obstacles such as firewalls, network address translation (NAT), and others, which make it hard to communicate [9].
- An architecture is required for scalability as there are billions of devices already, and it is growing tremendously where these devices are communicating all the time, which raises the need for a Highly Available (HA) approach that helps deployment across data centers to enable disaster recovery [9].
- Some devices are designed for everyday use, and they do not have user interfaces so, there is a need to maintain automation as well as to manage updates and to manage these devices remotely [9].
- A model is needed to manage the integrity and access control for IoT devices. Because of collecting and analyzing the data, IoT devices are generally used, and also the data they distribute and consume is the essential requirement [9].

However, the main goal is to provide an architecture that maintains integration between systems and device [9]

1.5.1 IoT reference architecture requirements

There are some requirements for IoT reference architecture that are unique and important. For instance, devices can be different from the manufacturer, and they can be unique in specifications or power factor. In other factors, some devices are traditional, and they need to connect to the new

devices with the latest technology, which can be a difficult task. Therefore, the number of crucial practices is utilized so that these devices can work together and give high performance [9].

For that, there are some requirements which are categorized following for IoT architecture:

1. Connectivity

In many devices, protocol, namely HTTP, has a significant place. A small device with an 8-bit controller can create simple GET and POST requests where HTTP provides important uniform connectivity. Although some traditional internet protocols and the overhead of HTTP can be a concern for two reasons. First, the memory size of the program is significant, and that can create a problem on small devices. But the biggest problem is the power requirements. A simple, short, and binary protocol are needed to complete these requirements. Another condition is the strength to cross the firewalls. Moreover, these devices connect directly as well as through gateways [9].

Two protocols are required for the devices that connect through a gateway. First, to connect to the gateway and second from the gateway to the cloud [9].

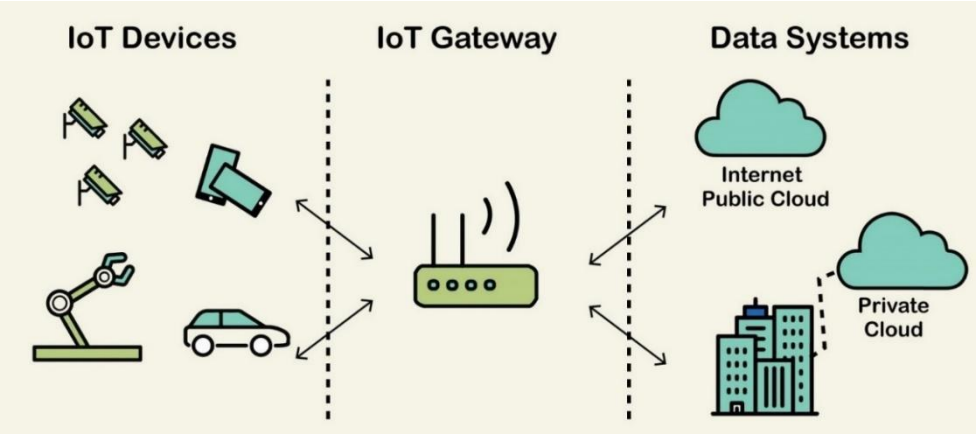


Figure 13. IoT devices connecting via a gateway

Source: https://www.lanner-america.com/wp-content/uploads/107-2.jpg

The IoT gateway gets these transmission modes and data protocols, and it can explain them to the other protocols that are required by the data systems.

In the end, in IoT architecture, there is a need to support transport and protocol bridging [9].

2. Device Management

IoT devices may need software updates or bug fixes until installed. After some time, it has to be repaired or replaced, which can result in downtime. To solve this problem or to manage IoT devices, IoT Device Management can be used [11].

It is the method for authentication, configuration, monitor, provision and manage the software and device firmware that gives its functional capabilities. Besides, security, health, and connectivity of the IoT devices are the main factors, and to maintain it, effective device management is vital [11].

Some Requirements for IoT Device Management:

Four basic requirements need for the IoT Device Management, which is as follow:

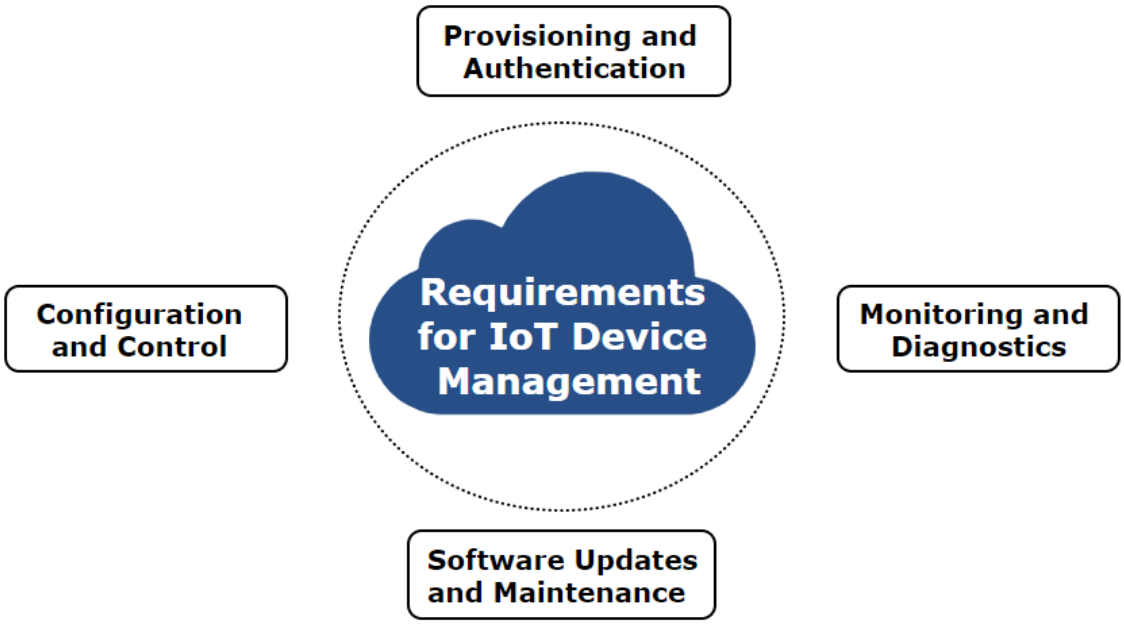


Figure 14. IoT device management

Source: https://www.educba.com/iot-management/

- Authentication and Provision:

Authentication means a process that only enrolls devices with legitimate credentials. Every device which installs will have the certificate or key to check its authentication. When the latest device

deploys, it will be authenticated by valid credentials and unique model number, serial number, and many more [11].

The provision means a process through which a device enrolls in the system. It has two parts;

I. The demonstration of an initial connection between a device and an IoT device done by registering the device [11].
II. A configuration performs on the device based on the requirements of the solution [11].

The device is wholly provisioned after completing these steps only.

- Configure and Control:

While installing a new device, some configuration should be done before starting to use it. For instance, a new device such as "a location tracker" is installed in a car. And the data is uploaded every minute in the cloud. However, before starting to use the device, specific device settings, including car number, car speed, and car driver name, have to be completed; unless, confusion will create. It can create a problem if this step is not completed before start using the car [11].

Still, some critical issues can be formed in certain aspects like functionality, performance, and security issues. Therefore, to reset the device to factory configuration is advised before decommissioning them. Devices can reset remotely to recover from errors, and this can help implement control capability in the system [11].

- Monitor:

To solve issues such as software bugs or other problems that can result in downtime of devices, a user must confirm it first, and for that, continuous monitoring is necessary. The software with device management can continuously diagnose the issues by logging [11].

- Software update and Maintenance:

After the installation, an update is essential for the perfect working of the device, and some additional functionalities will also include. However, it is tough to update all the devices manually as the number of devices is increasing every day [11].

Hence one of the most critical components of effective device management is the capacity to update and maintain remote device software securely, and these are the requirements that should be offered by an IoT architecture [11].

3. Data Collection, Analysis, and Actuation

Most of the IoT devices mainly focus on offering sensors or actuators or a combination of both, and only some of the devices have some form of User Interface [9].

The IoT reference architecture is built for the operation of a vast number of devices. If these devices generate constant data streams, then this produces a significant amount of data [9].

The requirement is for a storage system that is highly scalable and can handle various data and high volumes [9].

Furthermore, the device must be able to analyze data and operate on it. More powerful engines can be utilized for event analysis and operation on more powerful devices [9].

4. Scalability

Ideally, every server-side architecture would be highly scalable, supporting millions of devices that are continuously sending, receiving, and acting on data. However, many "highly-scalable architectures" are very costly both in hardware and software, also very complex [9].

For this architecture, an essential requirement is to maintain scaling from a small deployment to a vast number of devices. In contrast, flexible scalability and deployability are vital in a cloud infrastructure [9].

An essential requirement for making this an affordable architecture for small as well as large deployments is the ability to scale the server-side out on small and cheap servers [9].

5. Security

Security is the vital element of IoT, where IoT devices are collecting highly personal data often. Moreover, these devices are bringing the real world onto the Internet, and vice versa [9].

However, it also carries the risks that have three categories, such as:

1. The inherent risks in the internet system but are not known to IoT or product designers.
2. Some specific risks that are different for IoT devices.
3. For instance, safety to ensure no harm is due to the misuse of actuators.

The first category includes simple things like locking open ports on devices, for example, the internet-attached fridge, which had an unsecured SMTP server and was used to send spam [9].

The second category covers the concerns mainly related to IoT hardware, where the device might have its secure data read. For example, many IoT devices do not support proper asymmetric encryption because of their too-small size [9].

And the third category, Identity, and Access Management are the two critical issues for IoT security. Identity is a problem where poor practices are implemented. A common mistake is to use clear-text passwords within devices and machine to machine. Therefore, security requirements should support [9]:

- ✔ Powerful encryption on devices.
- ✔ A modern, token-based identity model should be used rather than user IDs and passwords.
- ✔ Keys and tokens management as smoothly and remotely as possible.

This concludes the set of identified requirements for the reference architecture. Any given architecture, of course, can add additional requirements. While some requirements may be met by the architecture and others may require additional components to be added. Nevertheless, the specifications are for a modular architecture that encourages extensions, dealing with demand [9]. I will discuss the architecture and approach in the next section.

1.5.2 The Architecture

The IoT reference architecture consists of a set of components. It consists of multiple layers, and each layer explains with terminology that can be standardized to create a reference framework that is accepted globally [10]. There are also some vertical layers, such as Device Manager and Identity & Access Management. Moreover, these layers will be discussed in the following sections;

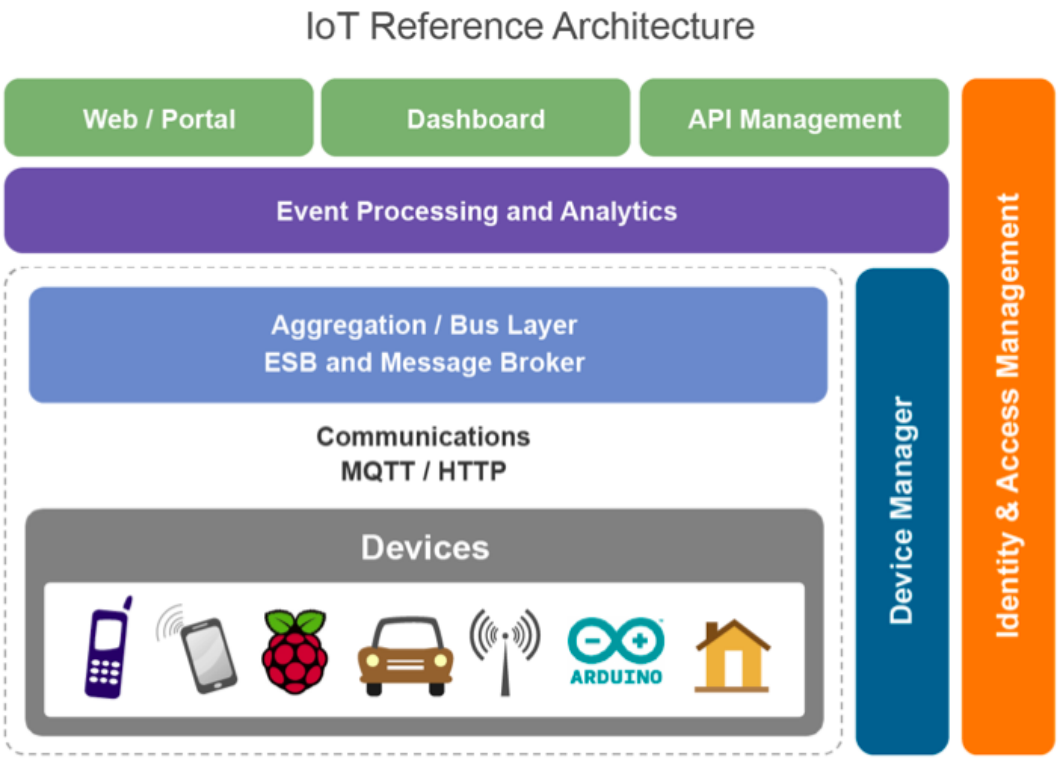


Figure 15. IoT reference architecture

Source: https://dzone.com/articles/internet-things-iot-reference

The layers are as follows [9]:

1 The Client and External Communications Layer - Web / Portal, Dashboard, API Management.
2 The Event processing and Analytics layer (data storage).
3 Aggregation and Bus layer - ESB and message broker.
4 The Communication Layer - MQTT or HTTP.
5 The Device Layer - IoT devices.

Other vertical layers are as follow:

6 The Device Manager.
7 Identity and Access management

1 The device layer

The IoT Reference architecture starts with the bottom layer, which is a device layer. These devices can be of many types and might control multiple devices. The Things in the IoT include a wide range of endpoints devices that can transfer and accept the data. However, to be considered as IoT devices, they must have certain communications, which is either a direct or indirect connection to the internet [9].

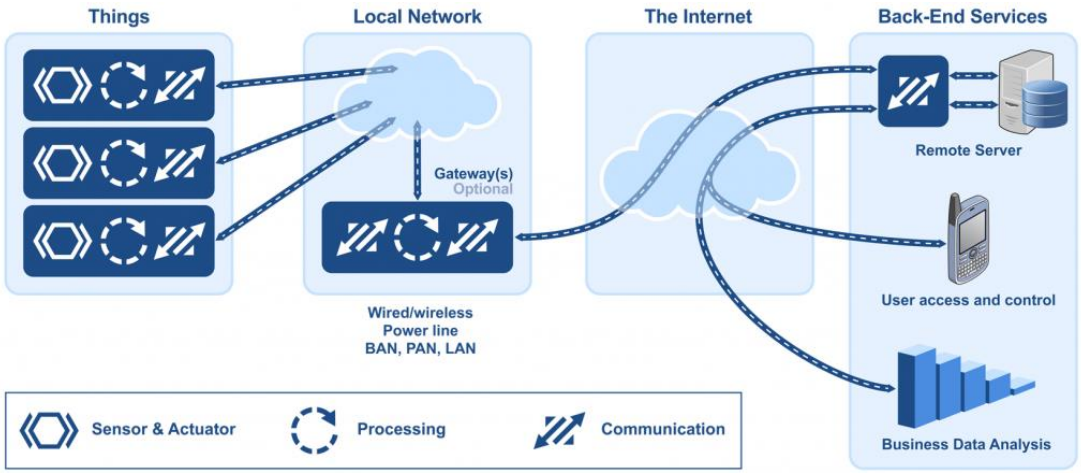


Figure 16. IoT device communication

Source: https://www.micrium.com/wp-content/uploads/2014/03/internet-of-things-1024x438.png

Some examples of direct connections are [9]:

- Raspberry Pi connects through Ethernet or WiFi.
- Arduino connected via Ethernet connection (Arduino).
- Intel Galileo connected through WiFi or Ethernet.

Some examples of indirect connections are [9]:

- Mobile phones connected through Bluetooth.
- ZigBee Gateway is used to connect ZigBee devices.
- Devices communicate with a Raspberry Pi through low - power radios.

Moreover, each device requires an identity that might be one of the following [9]:

- A unique identifier burnt into the device which can be the part of the system-on-chip or provided by a secondary chip.
- A UUID is produced by the radio subsystem like Bluetooth identifier and WiFi- mac address.
- EEPROM: an identifier that is stored in non-volatile memory.

It is recommended that every device has a UUID, which is an unchangeable ID given by the core hardware for the reference architecture. Also, some devices can be the size of a silicon chip, or some can be as large as a vehicle [9].

2 The communication layer

The second layer at the bottom is the communication layer. This layer supports the connectivity of the devices. There are several potential communication protocols between the devices and the cloud [9].

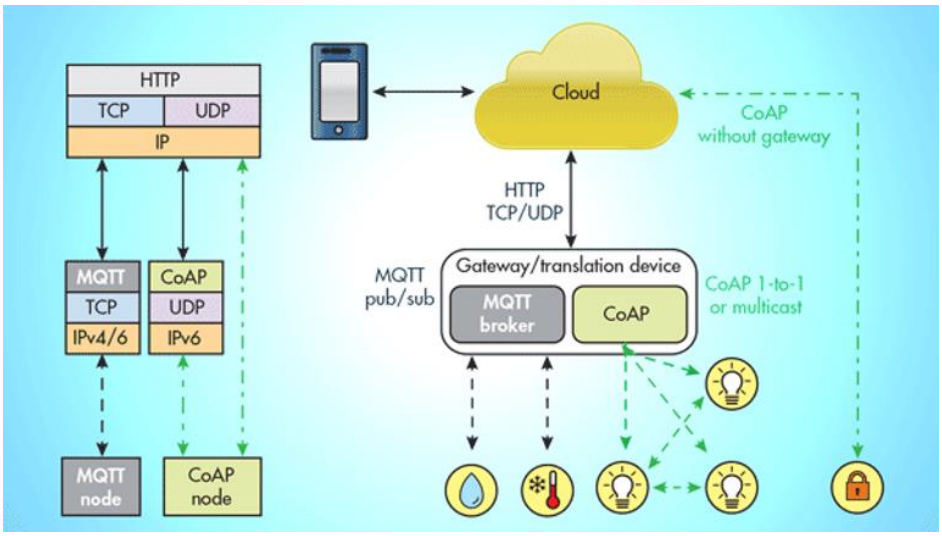


Figure 17. Connectivity using the different protocols

Source: https://www.electronicdesign.com/technologies/iot/article/21800998/mqtt-and-coap-underlying-protocols-for-the-iot

Three most well-known protocols are [9]:

I. HTTP/HTTPS (Hypertext Transfer Protocol)

II. MQTT (MQ Telemetry Transport)
III. CoAP (Constrained application protocol)

Let's briefly define these protocols.

I. HTTP/HTTPS is renowned, and there are so many libraries that support it. It is a simple text-based protocol, and many small devices can only partially support the protocol [9].
II. In 1999, MQTT was invented to solve problems concerning embedded systems and SCADA. It has two old versions (3.1) and the current version (3.11). MQTT protocol designed to help lossy and intermittently connected networks and also designed to flow over TCP. It has a minimal overhead that is only 2 bytes per message [9].
III. CoAP is based on the traditional client-server approach rather than a brokered approach and is designed to be used for UDP. This protocol is from the IETF and was intended to give a RESTful application protocol on HTTP. It is with a smaller footprint and has a binary approach rather than a text-based approach [9].

However, for this reference architecture, MQTT is selected as a preferred device with HTTP as an alternative option for the communication protocol.

MQTT is selected because of the following reasons:

- More extensive library and Better adoption for MQTT.
- Evident bridging into existing event collection and event processing systems: and
- Connectivity over firewalls and NAT networks in a simple way.

Besides, connectivity includes [10]:

- Communication with and between layer one devices.
- Reliable delivery beyond the networks.
- Multiple protocols implementation.
- Routing and Switching.
- Translation among protocols.
- Network-level security.
- Network Analytics (Self Learning)

There is one crucial feature with IoT devices, as they are not just to send the data over the cloud or the server though also the reverse. The advantage of the MQTT specification usually avoids firewall problems only because this approach works behind firewalls or through NAT [9].

When the communication is based on HTTP, mainly, which is a traditional approach for sending the information to the devices would be by using HTTP polling. That is very inefficient and costly both in terms of network traffic and power demands. Although modern replacement is available for this is the WebSocket protocol, which supports an HTTP connection to get upgraded into a duplex connection (full two-way connection or communication) and act as a socket channel between the client and the server. After establishing it, then the system can choose the continuing protocol to tunnel over the connection. But there is one disadvantage of this protocol. It can be used only on the larger 32-bit devices [9].

3 The aggregation and bus layer

The third layer from the architecture is the aggregation layer. It is an essential layer of the architecture that aggregates and brokers communication. It an important layer because of the following reasons [9]:

- The ability to help an HTTP server and an MQTT broker to talk to the devices.
- To route communications to a specific device possible via a gateway and the ability to aggregate and combine communications from distinct devices.
- The ability to bridge and transform among distinct protocols.

This layer not only provides these capabilities but also adapts to legacy protocols. Whereas, the bus layer can also offer some simple correlation and mapping from various correlation models. For example, a device ID mapped into an owner's ID or vice-versa [9].

Finally, two key security roles must be fulfilled by the aggregation/bus layer. It should be able to function as an OAuth2 Resource Server. It should also be able to work as a policy enforcement point (PEP) for policy-based access. In this architecture, to validate access requests, the bus requests to the identity and access management layer. Further, in this process, the identity and access management layer acts as a policy decision point (PDP). Then the bus layer implements the effects of these calls to the PDP to approve or reject the resource access [9].

In addition, it also includes:

- Data filtering, cleanup, and aggregation.
- Inspection of the packet content.
- Thresholding; and
- Event generation.

4 The event processing and analytics layer

This is the fourth layer of the architecture. This layer collects the events from the bus and gives us the ability to process certain events and act upon them. The main feature here is the need to store the data in a database. It can happen in two ways [9]:

- The first approach is to use a big data analytics platform. It is a cloud-scalable platform that promotes technologies like Apache Hadoop to implement a highly scalable analysis of the incoming data from the device.
- The second approach is to help the complex processing of events to start real-time activities and action based on data from the devices and the system.

In this step, the recommended approach is using the following strategies [9]:

- For storing the events, highly scalable, and column-based data storage.
- Map-reduction for long-running data processing.
- Complex event processing based on data and activity of devices. Other systems for fast in-memory processing and real-time reaction and autonomic actions.
- Besides, this layer can also support traditional application processing platforms like Java Beans, message-driven beans, or alternatives like PHP, Ruby, or Python.

5 The client and external communications layer

It is the fifth layer from the bottom in the reference architecture. Where the reference architecture must provide a way for these devices to connect outside the device-oriented system [9]. It includes three key strategies which are as follow:

- First, it needs to be able to create web-based front ends and portals that communicate with devices and the event-processing layer.
- Second, it needs the ability to design dashboards that give insights on analytics and event processing.
- Finally, by using machine-to-machine communication (API), it must be able to interact with systems outside this network. Whereas it is necessary to manage and control these APIs, and this happens as an API management system.

Moreover, a modular front-end architecture such as a portal (that allows simple, fast composition of useful UIs) can be utilized to build the web front end, which is a recommended approach. Also, this architecture supports existing Web server-side technology like PHP, Ruby, JSP/ Java Servlets, and many more. The suggested approach is based on the Java framework, and the most popular Java-based web server is Apache Tomcat [9].

The dashboard is a reusable system that aims to create graphs and other simulations of data coming from the sensors and the event processing layer [9].

On the other hand, the API management layer provides three main functions:

- Firstly, it offers a developer-focused platform that allows developers to find, explore, and subscribe to APIs from the system.
- Secondly, the gateway manages access to the APIs, implements access control checks (for external use), and throttles policy-based usage.
- Third and the last, the gateway publishes data in the analytics layer where the data is stored and analyzed to provide information into how the APIs are used.

6 Device Management (DM)

The device manager layer is one of the vertical layers from the reference architecture, where two elements handle the device management. A server-side system (the device manager) communicates with devices through different protocols and offers control both individual and in bulk devices. It also manages software and applications which are deployed on the device remotely, and if required, the device can be locked or wiped [9].

The device manager works alongside the device management agent. There are several agents for different types of platforms and devices [9].

Besides, the device identification list must be maintained and mapped into owners by the device manager. In order to manage access control over devices, it must work with the identity and access management layer. For instance, who else, apart from the owner, will manage the device, and how much control the owner has vs. the administrator [9].

Three levels of devices include non-managed (NM), semi-managed (SM), and fully managed devices (FM).

I. Fully managed devices: Fully managed devices are those who run a full device management (DM) agent. It supports the following [9]:
   - Manage the software on the devices.
   - On or off device features such as camera, hardware, and so many.
   - It manages the security controls and identifiers of devices.
   - Monitor the device's availability.
   - Keep a record of the location of the device, if possible.
   - Remotely lock or wipe the device when the device is compromised.

II. Non-managed devices: In non-managed devices, there are no agents involved, and it can communicate with the rest of the network. It might use 8-bit devices where the constraint is minimal to support the agent. If accessible, the device manager may keep information about the device's availability and location [9].

III. Semi-managed devices**:** Semi-managed devices are the ones that implement a particular part of the device manager. For example, features control but not software management [9].

7 The identity and access management layer

The final step of the reference architecture is the Identity and access management layer. This layer must provide the following services [9]:

- OAuth2 token issuing and validation (to authenticate API)
- Some other identification services that include SAML2 SSO and OpenID connect support to recognize web layer inbound requests.
- Extensible Access Control Markup Language (XACML PDP)
- User directory (for example, Lightweight directory access protocol)

For an instantiation of the reference architecture, the identity layer may, of course, have other specific requirements relevant to the other identity and access management. In this section, we outlined the main components of the reference architecture and the specific decisions that we took about the technologies. The specific requirements of IoT architectures and best practices to build agile, evolving, scalable Internet architectures drive such decisions [9].

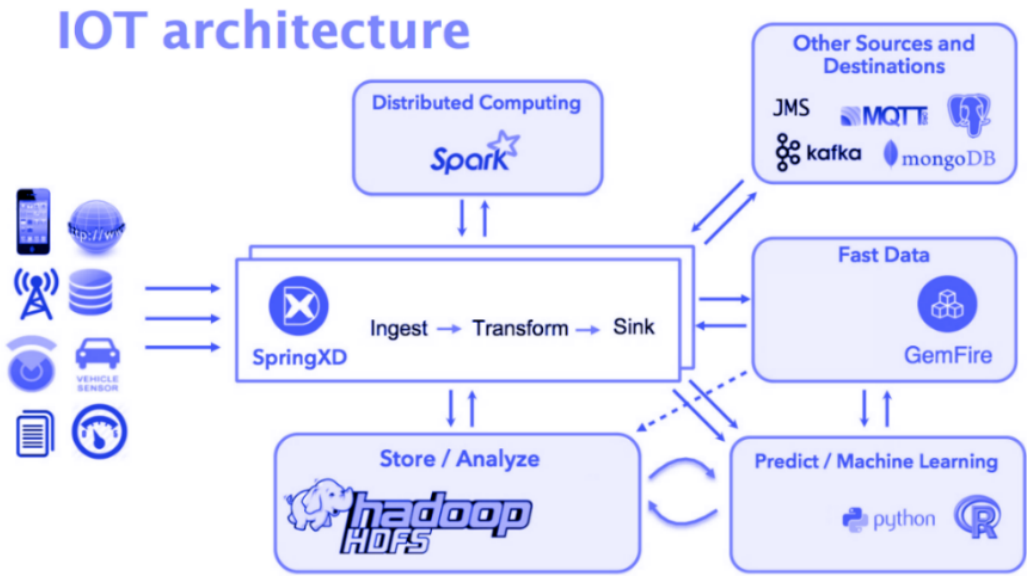


Figure 18. IoT architecture

Source: https://d2h0cx97tjks2p.cloudfront.net/blogs/wp-content/uploads/sites/2/2018/06/IOT-ARCHI-IMAGE-1.png

Although there are some other options available too, this reference architecture uses tested strategies that have proven to be effective in real-life IoT projects [9].

1.6 IoT protocols

The IoT communication protocols are the communication modes that secure the data being transferred among connected devices, and it also assures maximum protection [12].

Usually, the IoT devices are connected to the internet through an IP (Internet Protocol) network, although devices such as Bluetooth and RFID enable local connection to IoT devices [12]. While connection via internet protocol networks is relatively complex, needing additional memory and power from the IoT devices where the range is not an issue [12].

Alternatively, the non-internet protocol networks need comparatively less power and memory. However, it does have a range issue [12].

There are two types of IoT Protocols:

1.6.1 Network protocols

It is used to connect devices over the internet. There are a set of communication protocols that are applied over the internet. And end to end data communication within the range of the network is enabled using IoT network protocols. Some of the communication or network protocols are explained following.

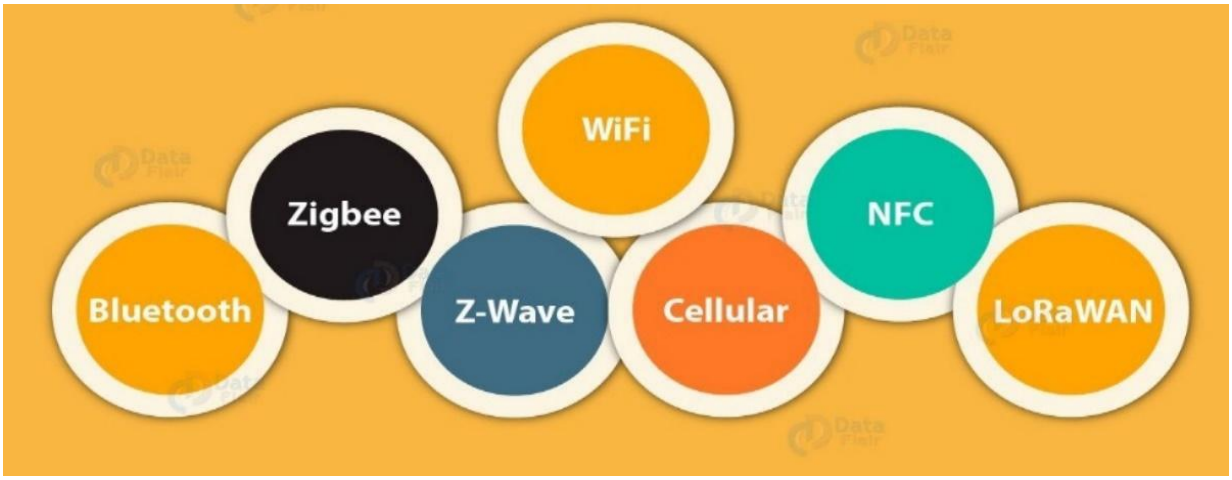


Figure 19. IoT network protocol

Source: https://data-flair.training/blogs/wp-content/uploads/sites/2/2018/05/IOT-Technologies-and-Protocols-01.jpg

I. Bluetooth:

Bluetooth is one of the important short-range IoT communications protocols [13]. It is a standard IoT protocol for wireless data transmission as well as has become essential in computing and many product markets [12].

This protocol is reliable and suitable for wireless communication between electronic devices with short-range, low-power, and low-cost. Bluetooth Low Energy (BLE) is a low-energy Bluetooth protocol version for IoT applications, which reduces power consumption as well as plays a significant role in connecting IoT devices [12].

Mostly Bluetooth protocol is utilized in smart wearables products, mobile phones, and other devices, where the data can be sent in small fragments without using high power and memory [12].

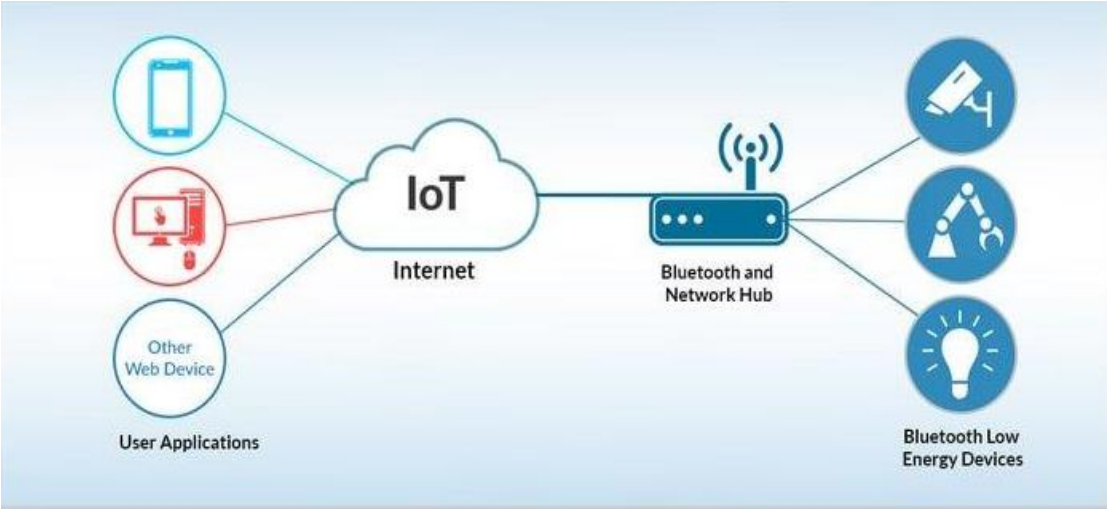


Figure 20. IoT network protocol - Bluetooth

Sources: https://www.ubuntupit.com/wp-content/uploads/2018/11/Bluetooth.jpg

II. ZigBee:

ZigBee is an IoT network protocol which is like Bluetooth. It supports smart objects to work together, and it is generally used in home automation [12].

It is majorly utilized in industries settings, with the applications that help low-rate data transfer between short distances [12].

For instance, the ZigBee communication protocol is used for street lighting and electric -meters in urban areas to provide low power consumption. It is also used in smart homes and security systems [12]

Figure 21. IoT network protocol – ZigBee

Source: https://i2.wp.com/www.iotleague.com/wp-content/uploads/2016/05/2016-ZigBee-Control-Your-World-e1463819625104.png?fit=310%2C400

III. Z-Wave:

Z-Wave is a wireless, radio frequency communications protocol that is mainly used in home automation to support smart devices such as lamp controllers and other sensors to connect and interact control commands and data with each other. This process works with two-way communication via mesh networking and message acknowledgment [14].

The Z-Wave protocol helps to mitigate power problems and gives cost-effective wireless connectivity to smart homes, presenting a low-power alternative to WiFi and a long-range alternative to Bluetooth [14].

Figure 22. IoT network protocol – Z-Wave

Source: https://www.the-ambient.com/media/images/2018/05/26349-postshomepage-preview-lg-1526369610-jXX3-column-width-inline.jpg

IV. WiFi:

WiFi is a wireless local area network (WLAN) that uses the IEEE 802.11 standard. It offers a range of hundreds of megabits per second, which is perfect for file transferring but can be too power-consuming for many IoT devices. Where one of the most popular IoT network (communication) protocols is the WiFi. Many developers often choose it, and mainly it has given the availability of WiFi inside the home environment within LANs. It offers fast data transfer, as well as the ability to manage a large amount of data. It provides many benefits, such as [13]:

- It gives universal smartphone compatibility.
- It is affordable.
- It is well protected and controlled.
- It is beneficial for many IoT devices to connect with an external cloud server.

However, there are some shortcoming as well:

- It relatively uses high power.
- Its instability and inconsistency.

Figure 23. IoT network protocol – WiFi

Source: https://www.ubuntupit.com/wp-content/uploads/2018/11/WiFi.jpg

V. Cellular:

Cellular communication protocol allows cell phone communication from one phone to the next about 10 to 15 miles antenna. Moreover, every IoT device that needs service over longer distances may take advantage of this cellular communication capabilities. Which are known as GSM, GPRS, CDMA, 2G, 3G, 4G / LTE, and EDGE based on the connection speed [13].

In IoT, this mode of communication is mostly related to Machine-to-Machine communication, as it allows devices like a phone to send and receive the data via the cellular network.

It can transfer a large amount of data using 4G, though the cost and power consumption can be too high for many IoT devices [13].

A cellular protocol can be excellent for sensor-based low-bandwidth-data designs, which will transfer the limited amount of data over the internet [13].

Figure 24. IoT network protocol – Cellular

Source: https://www.ubuntupit.com/wp-content/uploads/2018/11/cellular.jpg

It gives advantages such as stable connection, universal compatibility, and so many [13].

Also, it has some limitations, which are no direct communication from mobile phones to the device as it has to pass through satellite, very costly, and it uses high power [13].

VI. Near Field Communication (NFC):

Near Field Communication is a new and developing IoT network protocol, which is used in mobile IoT technology. It facilitates simple and secure communication among electronic devices, and especially for smartphones, supporting the user to carry out transactions where one does not have to be present in real.

It has expanded the contactless card processing functionality and allows the users to share the information at a distance less than 4 cm [13].

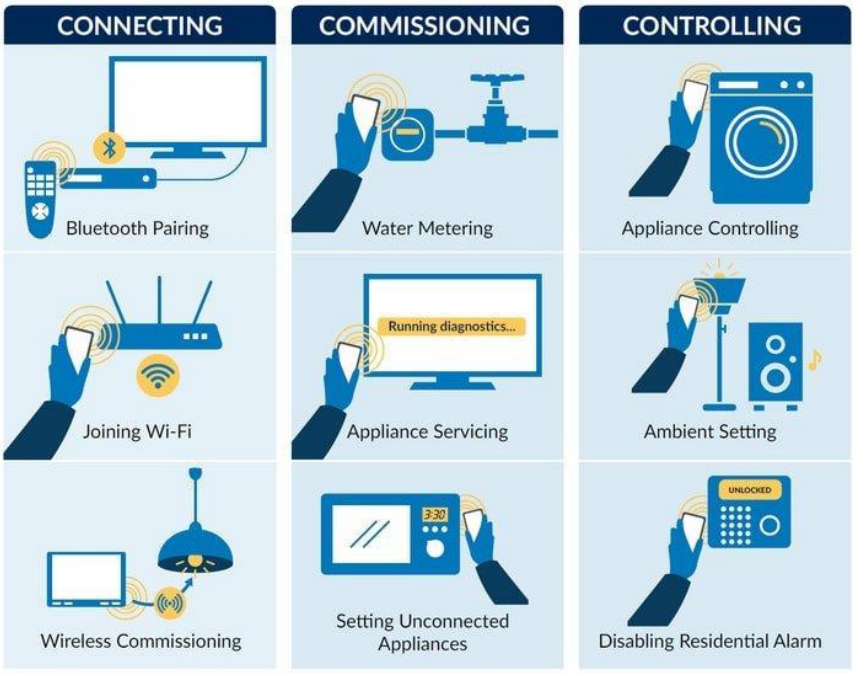


Figure 25. IoT network protocol – NFC

Source: https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/

VII. LoRaWAN:

It is a long-range and low power protocol that gives signal detection under the noise level [13]. It is one of the leading IoT technology which targets wide-area network devices [14].

It is intended to give low-power WANs with features needed explicitly in IoT, smart city, and industrial applications to support low-cost mobile secure communication. It specifically meets low power consumption requirements and maintains large networks with millions and millions of devices where the data rates vary from 0.3 kbps to 50 kbps [13].

This IoT communication protocol is used primarily by smart cities, where millions of devices function with less power and memory [14].

For instance, the practical use case of the LoRaWAN IoT protocol is smart street lighting. By using this protocol, the streetlights can be connected to a LoRa gateway. In turn, the gateway connects to the cloud application that automatically controls the intensity of light bulbs based on ambient lighting, which helps to reduce daytime power consumption [14].

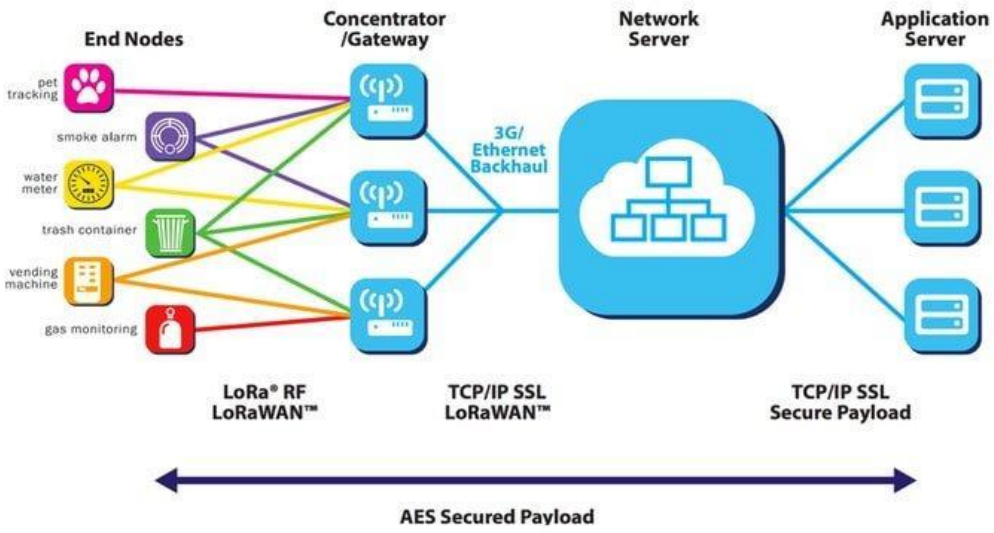


Figure 26. IoT network protocol – LoRaWAN

Source: https://www.ubuntupit.com/wp-content/uploads/2018/11/lora.jpg

1.6.2 Data protocols

The IoT data protocols are the one that is utilized to connect low power IoT devices. Such protocols provide point-to-point communication with the hardware at the user side without any internet connection. Also, in IoT data protocols, connectivity is through a wired or a cellular network.

Some important IoT data protocols are as follow:

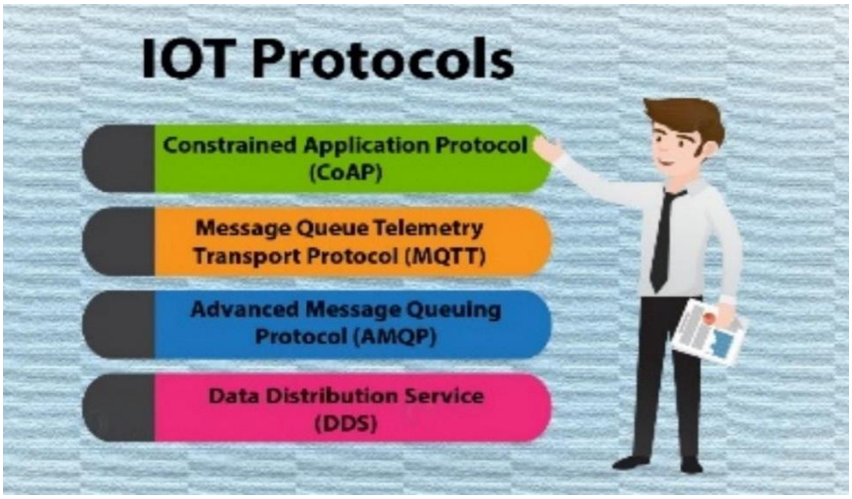


Figure 27. IoT data protocols

Source: https://d2h0cx97tjks2p.cloudfront.net/blogs/wp-content/uploads/sites/2/2018/06/IoT-Protocol.jpg

I. Constrained application protocol:

CoAP is an internet-utility protocol for constrained devices. Basically, it is used for Machine to Machine (M2M) communications where the client will send a request to the server, and then the server will send back the response in HTTP [13][14].

CoAP uses the UDP (User Datagram Protocol) for lightweight implementation and reduces space usage. It also utilizes restful architecture, like the HTTP protocol [13].

Mobile automation and microcontrollers are the primary examples of this, where the protocol sends a request to the endpoints of the application like appliances at home, which send back the responses of services and resources in the app [12].

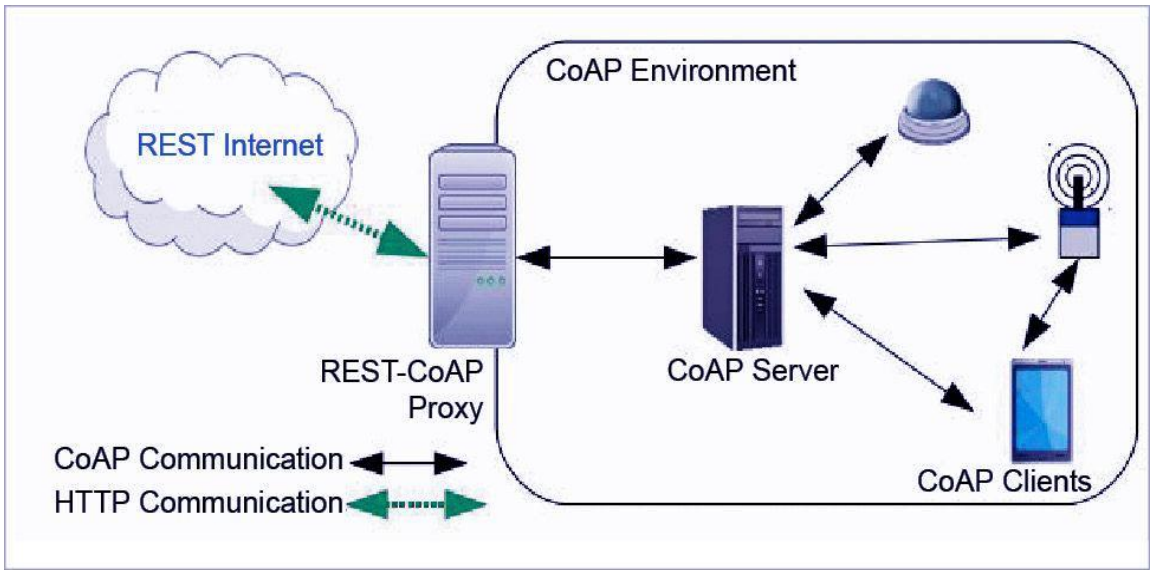


Figure 28. CoAP protocol

Source: https://d2h0cx97tjks2p.cloudfront.net/blogs/wp-content/uploads/sites/2/2018/06/IOT-PROTOCOLS-IMAGE-1.jpg

II. Message Queue Telemetry Transport Protocol (MQTT):

It is a messaging protocol developed by Andy Standford-Clark of IBM and Arlen Nipper of Arcom in 1999. It is designed for Machine to Machine communication, and it is one of the most preferred protocols for IoT devices.

MQTT gathers information from many electronic devices and helps remote device monitoring.

It publishes on the top of the Transmission Control Protocol (TCP) to support event-driven message interchange via wireless networks.

Furthermore, devices that are economical and need less power and memory use MQTT mainly.

III. AMQP:

Advanced Message Queuing Protocol (AMQP) is a software layer protocol, and John O'Hara developed it at JP Morgan Chase in London [13]. Generally, it is message-oriented and designed for middleware environments [15].

These IoT messaging protocols have been approved as an international standard as well as it contains hard and active components that route and save data (messages) within a broker carrier with a collection of policies for wiring the elements together [15][13]. It allows the patron program to communicate with the dealer and engage with the AMQP model [13].

AMQP IoT Protocol consists of three essential elements that can be linked into processing chains in the server to create the preferred capabilities which are as follows [13].

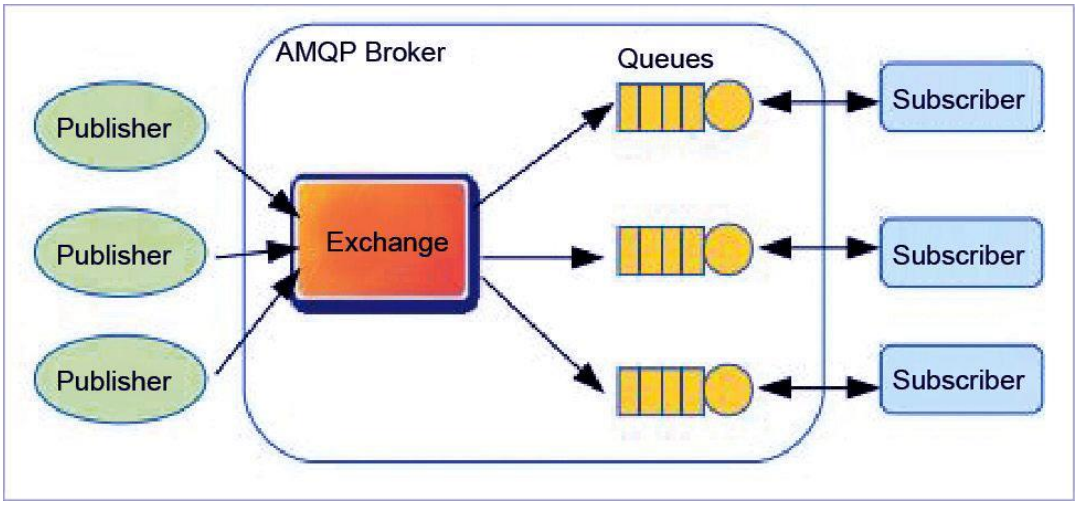


Figure 29. AMQP protocol

Source: https://d2h0cx97tjks2p.cloudfront.net/blogs/wp-content/uploads/sites/2/2018/06/IOT-PROTOCOLS-IMAGE-3.jpg

- Exchange: It receives messages from the publisher and then routes them to message queues [13].
- Message Queue: It stores the messages until the client software develops them [13].
- Binding: It works by connecting the message queue and the exchange [13].

IV. DDS:

Data Distribution Service is a high-performance standard, expandable, and real-time machine-to-machine communication among the internet of things protocols [15].

It is evolved and designed by Object Management Group (OMG), and with the help of DDS, data can be transferred in both low-footprint devices and with the Cloud platforms. Therefore, it is helpful to make use of multicasting to convey the high-quality quality of service to applications [13][15].

It comprises two significant layers which are the DCPS and the DLRL.

- DCPS: Data-Centric Publish-Subscribe is the layer that is worked by delivering the data to the subscribers [15].

- DCRL: Data-Local Reconstruction Layer works by giving an interface to the Data Public-Subscribe functionalities [15].

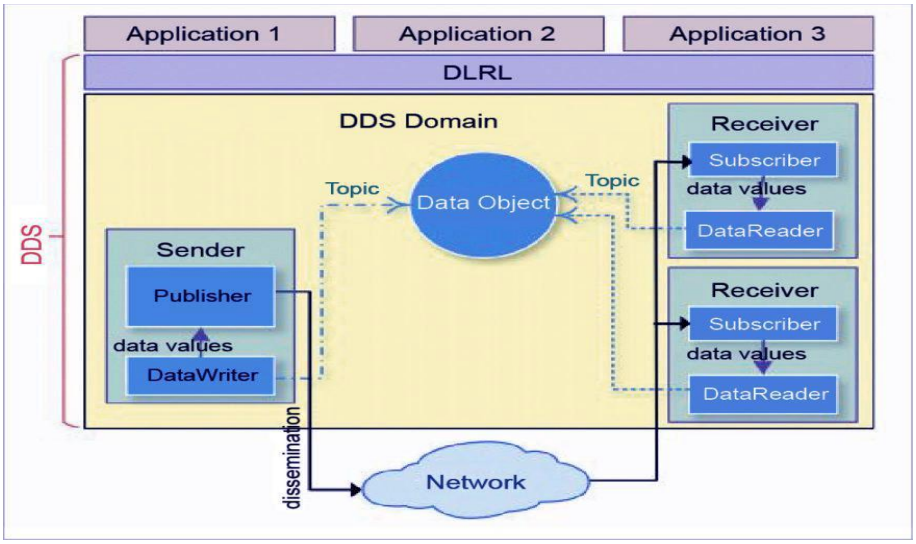


Figure 30. DDS protocol

Source: https://d2h0cx97tjks2p.cloudfront.net/blogs/wp-content/uploads/sites/2/2018/06/IOT-PROTOCOLS-IMAGE-4.jpg

1.7 IoT conclusion

The Internet of Things has offered so many exciting applications that make our lives much better and more comfortable in Healthcare, Transportation, Industries, and Agriculture.

IoT can transform everything and make devices able to be automatic without human interaction. Furthermore, the future of IoT is virtually infinite because of advancements in technology.

However, some issues, such as security, privacy, and data storage, should be considered to make IoT more beneficial, which will be discussed later.

1.8 What is a smart building?

Smart building refers to any structure which uses automated processes to automatically control the building environment and operations, including lighting, power usage, ventilation, security, and other systems [16] [17].

Undoubtedly, IoT based smart buildings have become very popular these days. It provides features like tracking and optimizing temperature, energy consumption, and occupancy in the building, and many more, which helps to improve the reliability and performance of the building [16] [17].

With the advancement of technology, building owners began to look outside of four walls and move towards integrated, more functional, and dynamic ways. Initially, the approach was more towards automation than intelligence, in which the first one involved the use of components solely to automate and simplify everyday tasks. Nevertheless, the second talks about extended algorithms where the systems can think and make decisions according to the user's needs, an extension of AI and Machine Learning [16] [17].

Figure 31. Smart Building

Source: https://fintk2.com/wp-content/uploads/2016/12/smartBuilding.jpg

Moreover, things are pointing up. Where the revenue links to sensor-equipped lightening installations, climate control devices, thermostats, and other automation systems cloud dramatically increase to around 732 billion dollars over the next decade, Navigant Research predicted in a report released in early December 2016 [16].

Furthermore, the first-ever built buildings were a simple structure made out of stones, sticks, animal skins, and other natural materials. Although they never resembled the steel and glass that make up a modern city skyline, the intention of these early buildings was the same to provide a comfortable place for the people inside [17].

Today buildings are complex concatenations of structures, facilities, and technologies. With time, each part within a building has been built and enhanced, enabling modern-day building owners to individually choose security, lighting, heating, ventilation, and air conditioning systems, as if they were constructing a home entertainment system [17].

Yet today, building owners begin to look outside the four walls to understand their building's effect on the electrical grid, their organization's purpose, and the global environment. To achieve these goals, it is not sufficient for a building to merely include the structures that provide comfort, light, and safety. Buildings of the future should link the different pieces in an integrated, dynamic, and functional manner. This dream is a building that fulfills its purpose effortlessly while reducing energy costs, maintaining a robust electric grid, and decreasing the impact on the environment [17].

At the most fundamental level, smart buildings offer essential building services that make the residents efficient (e.g., ventilation, environmental efficiency, air quality, physical security, sanitation, and much more) at the lowest cost and effect on the building lifecycle process. Achieving this goal includes adding intelligence from the very beginning of the design phase throughout the end of the building's useful life [17].

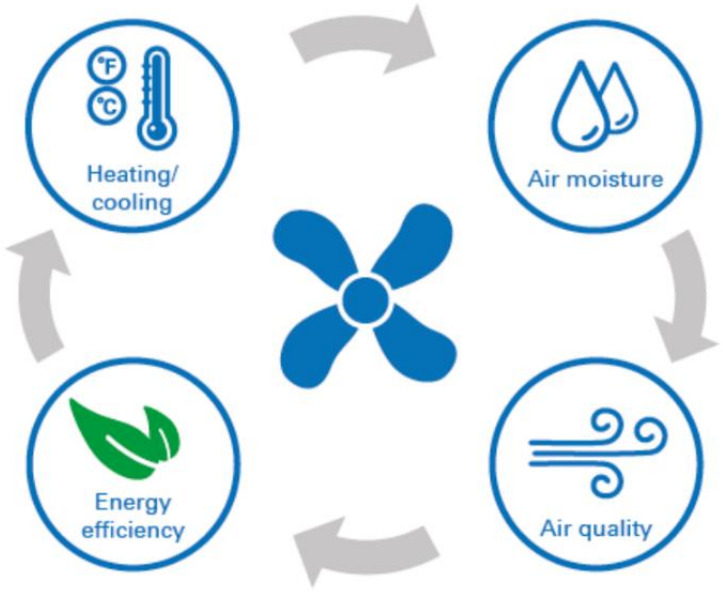


Figure 32. HVAC system

Source: https://www.tuv.com/content-media-files/master-content/services/industrial-services/0028-tuv-rheinland-ventilation-and-air-conditioning-systems/tuv-rheinland-ventilation-and-air-conditioning-systems-hvac-systems-visual-en_core_1_x.png

During the process, smart buildings utilize information technology to link several subsystems, which typically operate autonomously so that these systems can share data to improve overall building efficiency. Inside their four walls, smart buildings look beyond the building appliances. Where they are linked and responsive to the intelligent power grid, and they can communicate with building operators and tenants to provide them with a new level of visibility and actionable knowledge [17].

Supported by technology, this smart building integrates itself to the functions it exists to fulfill, which includes [17]:

i. To connect building systems.
ii. To connect people and technology.
iii. To connect to the bottom line.
iv. To connect to the global environment.

v. To connect to the smart grid.

vi. To connect to an intelligent future.

i. To connect building systems:

Modern buildings provide complex mechanical equipment, sophisticated control systems, and a range of facilities to improve occupant safety, convenience, and efficiency. Many of these programs require machine-to-machine interaction, but due to the general nature of the data and proprietary communication protocols, knowledge travels only along specific routes [17].

The smart building would need connectivity between all the building's equipment and systems. An example is chiller plant optimization, which improves chiller process output by incorporating external weather data and occupancy details [17].

Another example is the use of building security system data to shut off the lighting and minimize ventilation when there is no one present [17].

Moving towards interoperable, connected devices and systems within a building requires cooperation among many different parties, many of whom are historic competitors in the business. Notwithstanding the difficulty, over the past two decades, voluntary collaboration has contributed to the introduction of open standards such as BACnet, Modbus, and LonWorks, leveling the playing field by allowing each manufacturer and contractor to contribute to a functional whole [17].

As a result, a building where lighting, air conditioning, security, and other systems can freely pass data back and forth, which results in greater efficiency, more excellent safety and comfort, and lower facility operating costs [17].

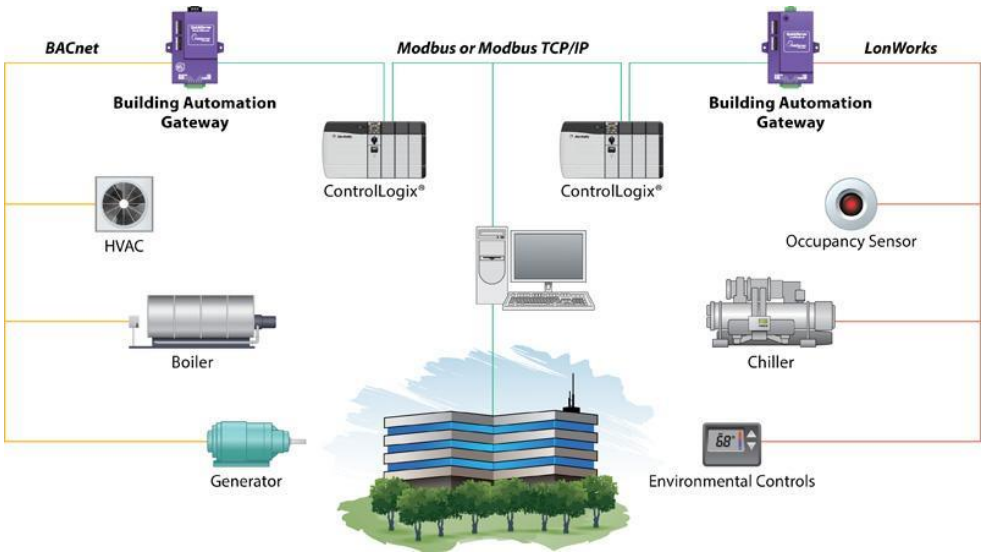


Figure 33. An example of open standards in smart building or building automation communications

Source: https://www.prosoft-technology.com/var/plain_site/storage/images/media/images/landing-pages/industrial-applications/industrial-automation-images/building-automation-diagram_web/62403-5-eng-US/Building-Automation-Diagram_web.jpg

ii. To connect people and technology:

Wires and transistors are the most sophisticated software and detailed hardware in the world without the people that use them to work more effectively [17].

In that respect, the people who run a smart building are a critical component of their intelligence. Despite low budgets and limited personnel, there is no space in modern-day facility management for hard training and steep learning curves [17].

Alternatively, a brilliant building offers interactive resources designed to improve and maximize the effort of the current people's on-the-ground. As the smart building emerges, it will provide the platform for innovation by sharing information among smart building systems and components [17].

Future applications may evolve when facilities managers engage with tools and technology to do their jobs better while offering more convenience, more safety within less cost, less energy, and less impact on the environment [17].

Figure 34. Connecting people and technology

Source: https://res.cloudinary.com/people-matters/image/upload/fl_immutable_cache,w_624,h_351,q_auto,f_auto/v1520777933/1520777931.jpg

iii. To connect to the bottom line:

A smart building is known as the "supersystem" of interconnected building subsystems. It compared the internet, which links computer networks into one bigger "supernetwork." The integration of systems can be utilized in a smart building to decrease operating costs [17].

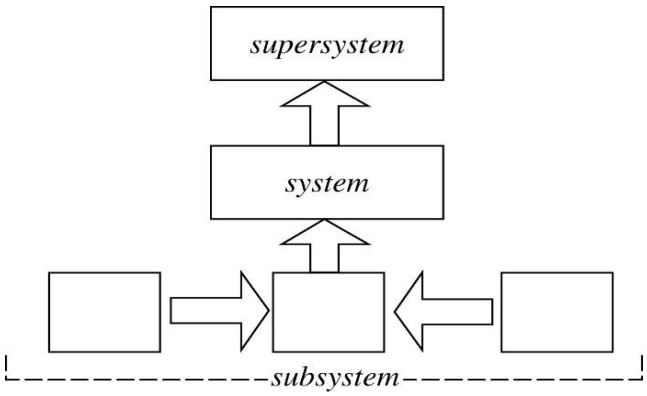


Figure 35. Supersystem connect with the subsystems

Source: https://royalsocietypublishing.org/cms/asset/6e9859ae-3694-4446-8c93-31468b17ca68/471fig1.jpg

A smart building can save money in a variety of ways which include optimized operation and increased efficiency [17]:

- Optimized cooling and ventilation systems: Dynamically designing loads allow the device to invest the minimum amount of money to provide the required level of comfort [17].
- Matching occupant trends to energy consumption: When there are fewer people inside, a smart building can operate leaner and save money [17].
- Proactive monitoring of equipment: Analysis algorithms will identify performance problems before they create expensive breakdowns, maintaining maximum productivity along the way [17].
- Dynamic energy consumption – A smart building guarantees the lowest possible energy costs. It often makes a profit by selling load reductions back to the grid by taking signals from the electricity market and adjusting usage in reaction [17].

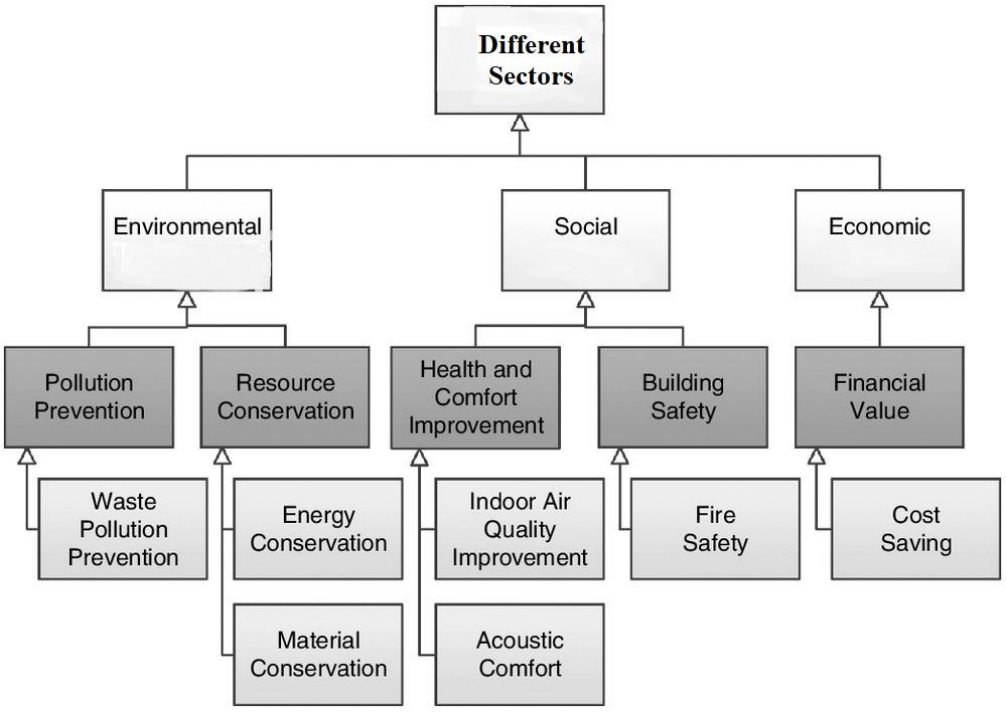


Figure 36. Different sectors where some operation should be applied to save money and energy in a smart building

Source: https://ascelibrary.org/cms/asset/a6d393a4-32f8-4a11-8c54-af3505a7d958/figure5.jpg

Open access to information is a platform on which it is possible to build significant value. A smart building provides a platform by connecting data in an open format, facilitating the development of new technologies that save time, resources, and operating costs, as well as the development of new web applications for the free information on the internet [17].

iv. To connect to the global environment

Building management systems have automated the cycle over decades for just supplying adequate electricity for heating and cooling buildings to fulfill comfort requirements. These energy-efficiency standards contribute to the environmental objectives of an enterprise, such as tracking and decreasing greenhouse gas emissions. But if the data become stuck inside the building management structure, decision-makers at the executive level cannot evaluate and operate on it [17].

Translation software named "middleware" captures data from all automated systems throughout an organization. Despite manufacturer or communication protocol and merges it into a standard platform for analytics and reporting. One consequence is the emergence of web-based dashboard displays providing a virtual overview of high energy usage facilities, unexpected maintenance costs, and many other circumstances that deserve prompt consideration [17].

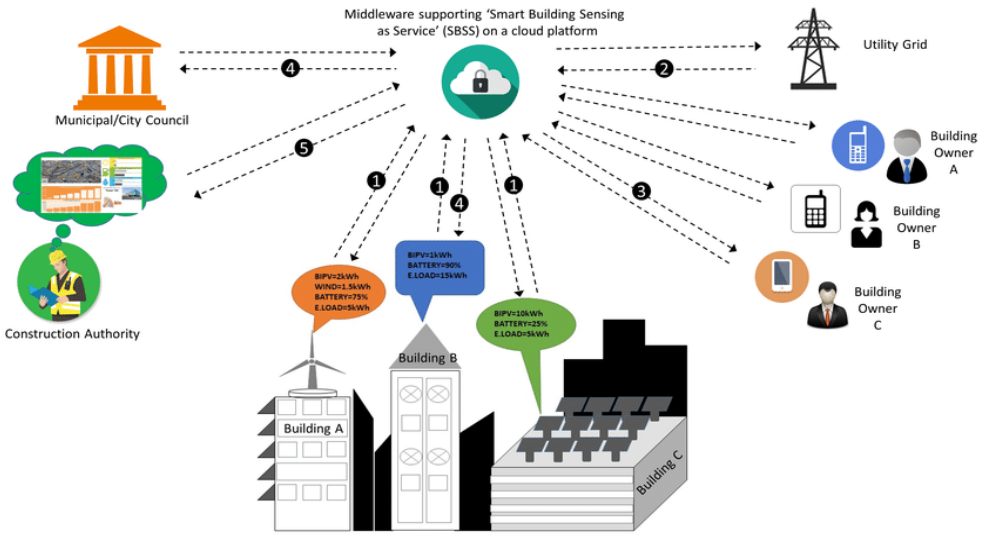


Figure 37. Middleware captures data from the automated system in smart buildings

Source:https://www.researchgate.net/profile/Clayton_Miller2/publication/328141398/figure/fig3/AS:680356080521219@1539220938971/A-future-scenario-Smart-Building-Sensing-as-Service-model-for-Cities.ppm

It brings clarity to managers in control of infrastructure and carbon footprint management to see their organization's big picture, no matter how many structures or geographical locations involved. While knowledge is quickly available and can be viewed everywhere, administrators can make better decisions that affect productivity instantly [17].

v. To connect to the smart grid

Especially smart buildings can take advantage of information that exists outside its walls and windows. The smart grid provides an ideal starting point. Electricity markets are moving into "real-time," implying that when wholesale prices elevate, or system stability is compromised, buildings can receive requests to reduce demand. Furthermore, effective electric rates are a rising trend, ensuring a building charges closer to the actual cost of producing power as soon as it is used rather than the average price over long periods [17].

For example, a smart grid system may be configured to read the weather forecast and expect an increase in temperature that will result in increased demand for the following afternoon. The utility could communicate an "offer" to pay $0.50 for each kilowatt-hour drop from its average power consumption to the smart building. A smart building could embrace this proposal by initiating an internal demand-reduction mode and thus reducing its price [17].

Although energy use and occupant satisfaction are essential to any enterprise and therefore require human participation in decision-making, technology will be the primary enabler, delivering the tools and information required by building managers to make smart decisions. Where facility managers are restricted as it is, the minimal response would be given to participating in an intelligent grid if operators were required to perform a "second job" monitoring markets and react to signals [17].

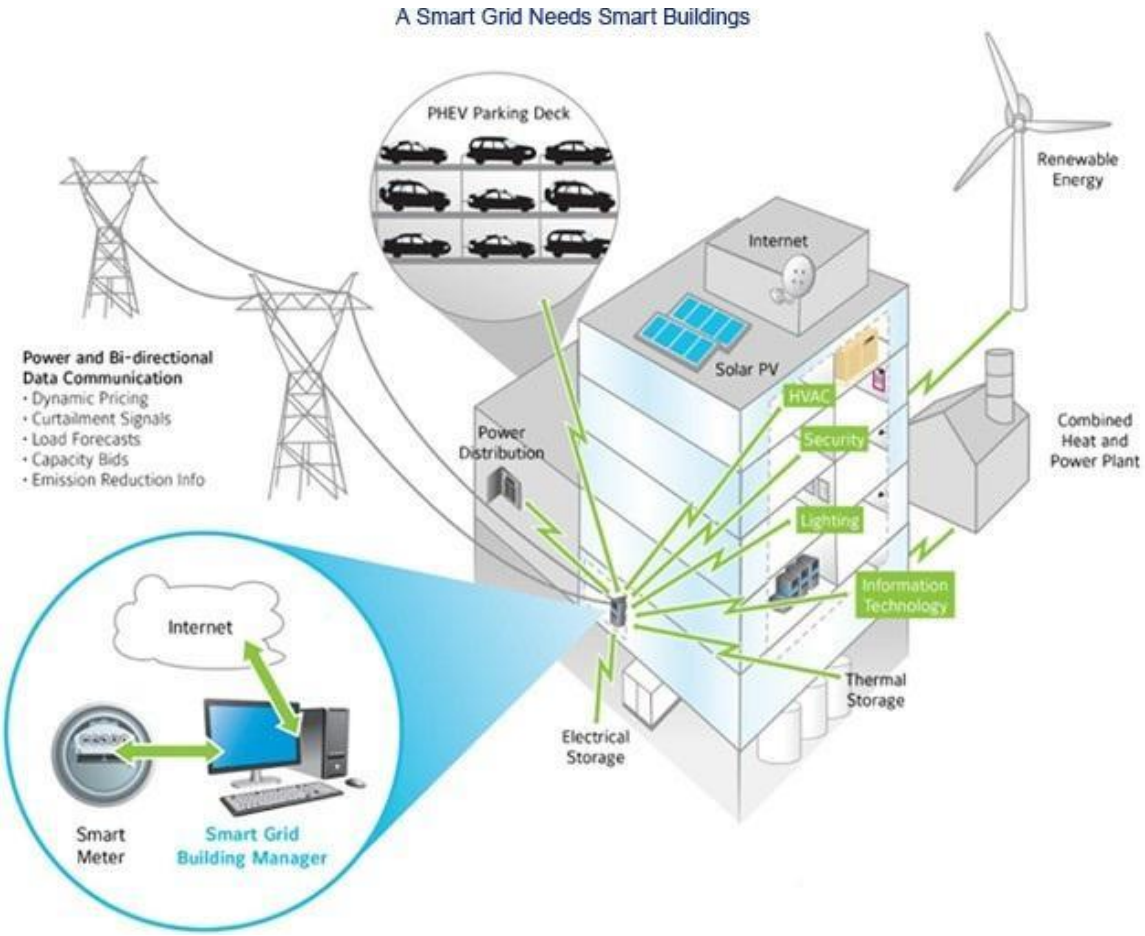


Figure 38. A smart grid in a smart building

Source: https://s3-us-west-2.amazonaws.com/buildingefficiencyinitiative.org/legacy/InstituteBE/media/Library/Images/Smart-Grid_Smart-Building/Smart-Grid_A-Day-in-the-Life-Illustration.jpg

vi. To connect to an intelligent future

Smart buildings go far beyond energy savings and contribute to sustainability objectives. They extend the life of industrial equipment and also have an impact on the safety and security of all resources, both human and mater. By creating a platform for accessing data, which allows creativity [17].

And through encouraging operators to shed electrical load and sell the "negawatts" into the marketplace, they transform buildings into automated power generators. It is a crucial component

of a society in which information technology and human ingenuity merge to create a future-proof sustainable low-carbon economy [17].

Furthermore, the advantages spread well beyond the smart building's four physical walls. The electrical grid is better and more efficient. The carbon footprint of the society is minimized as renewable energy sources provide the power, balanced with an information network that matches demand with variable supply minute by minute [17].

In a smart system, electric cars move people to residences and offices and act as moving batteries. Yet businesses are working at a higher level of efficiency by using data in new ways, leveraging the link between systems that have been entirely independent until now. Such incentives are not temporary but continue from modeling and design to renovation and beyond, throughout the entire life of the building [17].

The smart building is the center of this vision, providing not only the roof overhead but also the information infrastructure to make a possible brilliant world [17].

1.9 History and Evolution

Although smart buildings may seem like a rather modern concept their roots go quite far back in history. The first signs of an automatic HVAC system may have originated with Cornelis Drebbel in the 17th century. Drebbel developed a mercury thermostat, which could hold a room at a constant temperature automatically. His invention was one of the first historically known, feedback-controlled devices. He has also developed the first known air conditioning system, utilizing salt as a cooling agent. Then, in the 18th century, a French scientist, René Antoine Ferchault de Réaumur, built a temperature-controlled incubator based on the ideas of Drebbel and the thermometer discovered by Reaumur. The rise of digital computers in the 20th century was also an integral part of the advances of building automation technology, resulting in the modern building automation that we see nowadays [18].

Buildings use 39 percent of total energy consumption as the maximum of all energy consumption, as shown in Figure below. This portion of the building is the combined use of residential and commercial building consumption. Therefore, there are significant opportunities to make this building smarter and better control it and also communicate with end-users [19].

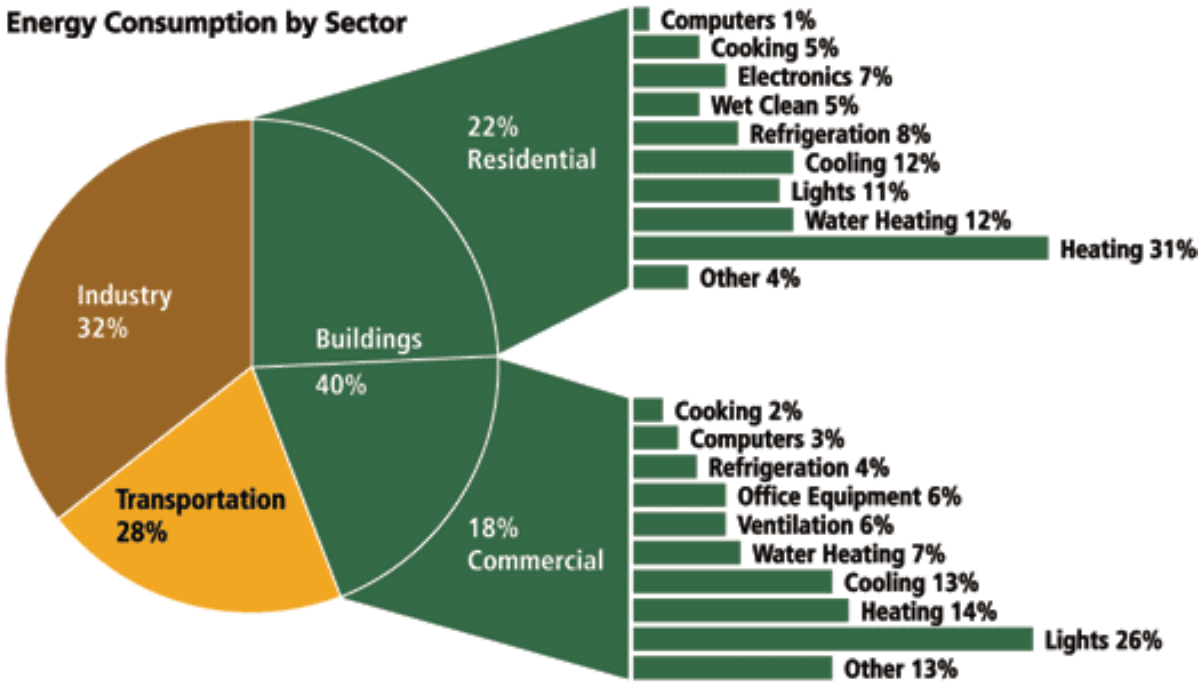


Figure 39. Energy consumption summary

Source: https://www.seas.ucla.edu/~pilon/images/PCM/BuildingEnergy.png

Since the 1950s, like most technologies, building automation has evolved just in our lives at a pace that would have confused facility managers and engineers. At that time, automatic buildings depended on pneumatic systems where compressed air was the medium of exchange for the monitors and controllers in the system [20].

By the 1980s, microprocessors had become small enough and cheap enough to be implemented in building automation systems. There was nothing short of a revolution of switching from compressed air to analog controls to digital controls [20].

A decade later, open protocols were adopted that enabled the controlled facilities to communicate with each other. Furthermore, by the turn of the century, Wireless technology authorized components to interact without cable connections [20].

Whereas, building automation and smart buildings technology have been skyrocketing since the beginning of the 21st century. The smart building technology industry continues to expand as increasing numbers of businesses and households see the advantages of adding energy-efficient

and sustainable systems to their structure. Currently, smart building infrastructure varies from automated and sophisticated HVAC systems to recognize security systems. Many of these functions can even be remotely managed from smartphones, tablets, and computers [18].

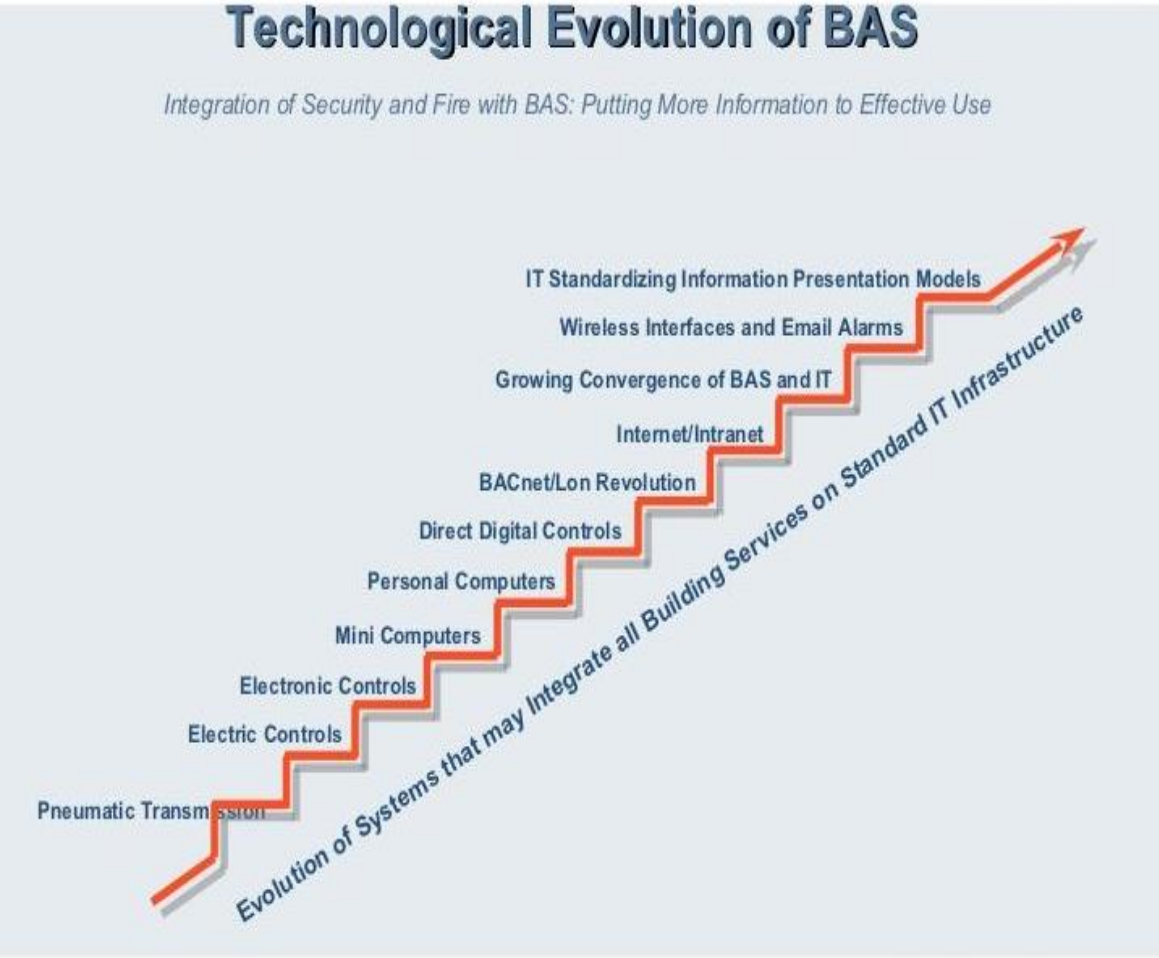


Figure 40. Evolution in building automation system / smart building

Source: https://image.slidesharecdn.com/ebtbuildingsecuritybriefing-1218725044564617-8/95/ebt-building-security-briefing-6-728.jpg?cb=1218700729

1.10 How does a smart building system work?

Building Automation System has five crucial components which are as follow [20]:

1. Sensors are the devices that measure states such as CO2 output, temperature, humidity, daylight, or even occupancy of the room [20].

2. Controllers are the mind of processes, where it takes information from the collector and then chooses how it will reply [20].
3. Output devices are the one that carries out the commands from the controller. For instance, sensors are relays and actuators [20].
4. Communications Protocols are the language that is spoken among the Building Autonomous System components [20].
5. The dashboard/user interface is the screens or the interfaces that are used by humans to interact with Building Automation Systems. Also, the dashboard is where data for the building is recorded [20].

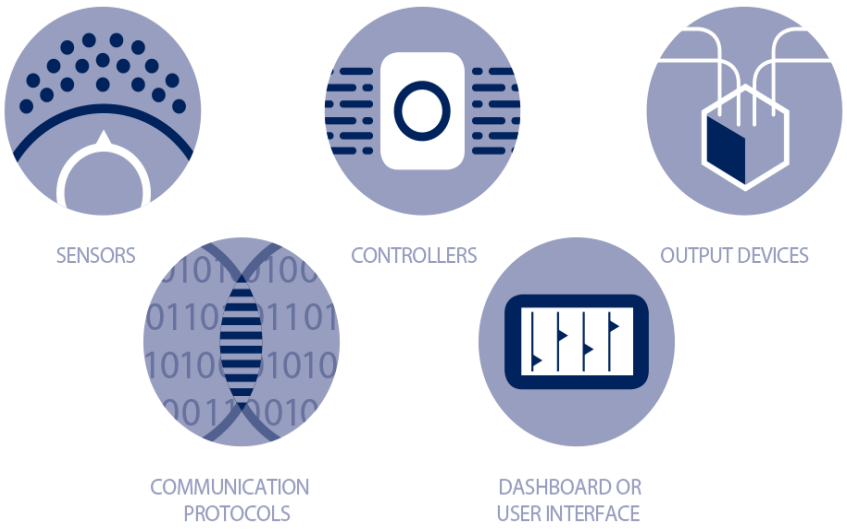


Figure 41. Components used in the building automation system

Source: https://controlyourbuilding.com/media/files/default/bas_systems.png

1.11 What can a smart building do?

1 The Lighting and HVAC devices can be set up to work according to a schedule that allows these systems both smarter and more effective [20].

2 Within a building, it can get the various components and equipment to collaborate and function together towards higher overall performance [20].

3 To manage the freshness, temperature, and comfort inside the building, it can maximize the flow of incoming outside air [20].

4 It can notify you when an HVAC unit operates in both heating and cooling, helping to reduce the expense of utility [20].

5 It can know when an incident like a fire breaks out and shuts off any equipment that might threaten the inhabitants of buildings [20].

6 It can identify an issue with one of the building's facilities, such as an elevator getting stuck with people inside and send an instant message or email to the facility manager of the building to alert him/her to the problem [20].

7 It can recognize who enters and leaves a building and when [20].

8 If any activity takes place, it can start a camera to do the recording and transfer a warning and direct video stream to the security team and facilities manager [20].

Figure 42. Smart building functions

Source: https://techaccess.co.ke/wp-content/uploads/2018/03/smart-building3.jpg

1.12 SB conclusion

Smart buildings "real value" is to make the building's data intelligible and create insights on top of that, eventually bringing those insights back into the business to optimize processes and interactions [21].

A smart building enables property owners to have better visibility in the health of the building, operators to be more proactive and to define more efficient processes. While the occupants benefit from interactive environments, excellent comfort, and gain higher efficiency [21].

2 Correlation between IoT and smart buildings

The Internet of Things (IoT) technology is a phenomenon that is rapidly evolving and fundamentally redefining nearly all markets and industries. The last five years have seen an inflection point where fragmented attempts to link devices and sensors in industry-specific ways now converge into an overall vision of connectivity permeating the global physical environment. With the rise of advanced technology, the smart building concept came into the scenario [22]. As the smart building industry is transitioning which can be seen in the figure below [23].

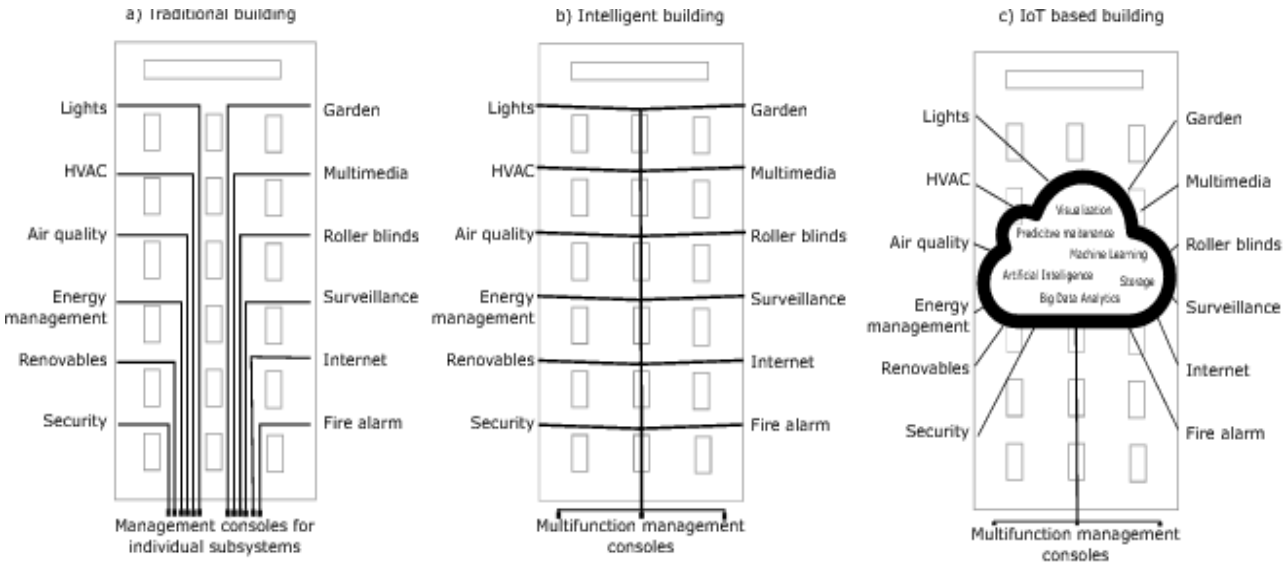


Figure 43. Transition in the buildings

Source: https://d3i71xaburhd42.cloudfront.net/ee837f49fdfc5ea7512a87443e25bad3eac4248c/1-Figure1-1.png

The internet of things is creating new ways for a race of smart building and also provides information that is more accurate and useful. However, the whole idea is about connecting everything to the internet [22]. In fact, many building industries are finding new ideas to utilize digital and intelligent infrastructure to optimize business value [23].

Companies working on smart infrastructure projects are automating the Heating, Ventilation, and Air Conditioning (HVAC) systems, the physical security of a building, energy usage, location software, as well as other areas of concern to building owners and their occupants [23].

Basically, building automation systems are projects of the internet of things (IoT), combined with automation and control. Sensors that track a local condition transfer the condition data to be processed through a high-speed network. Then the data will be used to initiate a decision and to act [22][23].

Furthermore, the cloud handles all data processing, which is necessary for many building automation systems. And with the internet of things, servers, analysis, and databases can shift into the cloud to have access to significant computing power for the analysis of the data, where most of the industries are heading nowadays [22][23].

The building blocks of building automation systems are sensors, controllers, and the server where the computing systems capture trends in the data created by the sensors and analyze it [23].

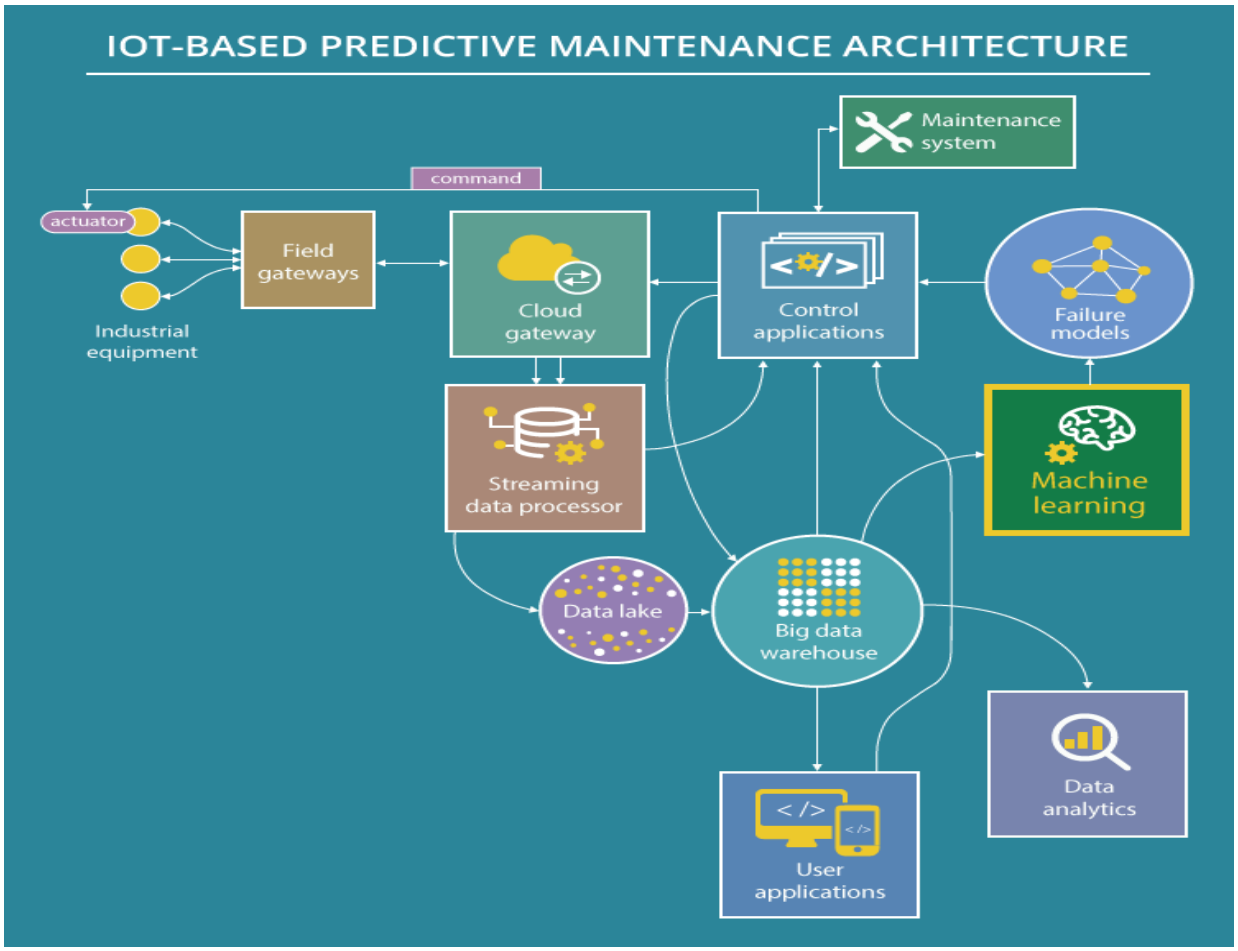
Figure 44. Features of a smart building

Source: https://i0.wp.com/semiengineering.com/wp-content/uploads/2018/10/IoT-for-Smart-Buildings.jpg?ssl=1

IoT has given many features into the smart building, which makes it more effective and intelligent, which are as follows [22]:

Predictive maintenance:

Predictive maintenance is a method that is used to assess the state of the machines in operation. Here, the focus is on two things, such as the prediction and the prevention of equipment failures in the future. Predictive maintenance utilizes the IoT devices to receive a report on the building under construction and all the equipment under operation. It gives a clear understanding of when maintenance is needed [22].



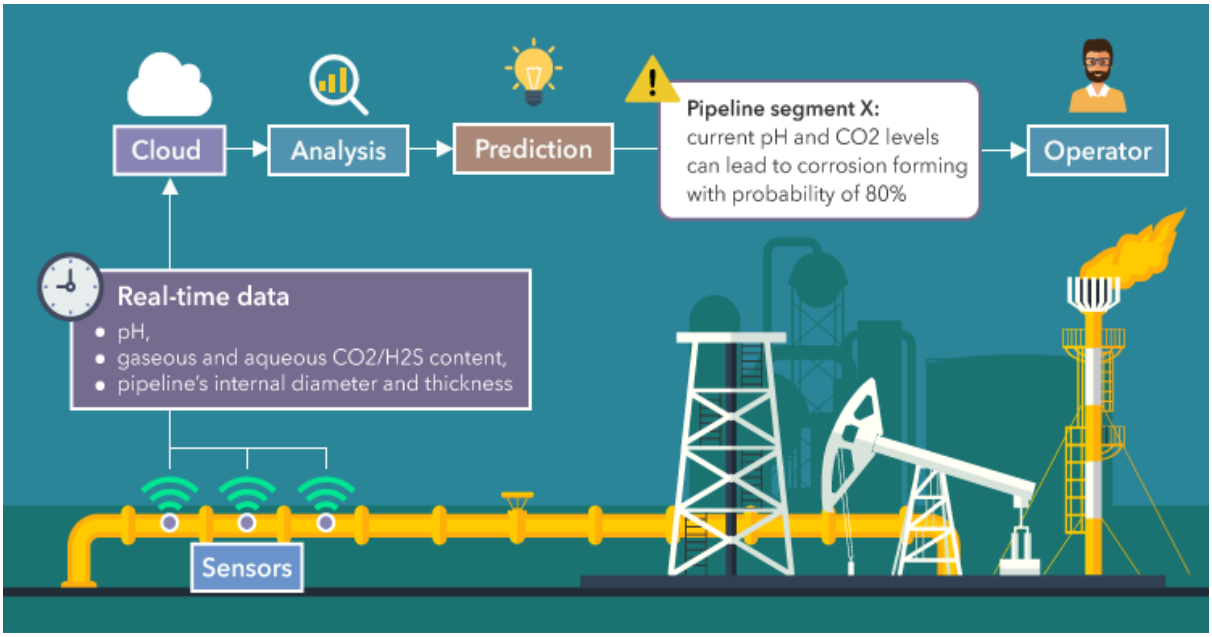


Figure 45. IoT based predictive maintenance alert system

Source: https://www.scnsoft.com/blog-pictures/internet-of-things/iot-for-predictive-maintenance-2.png

Hence, it reduces the time required for equipment maintenance. It also reduces maintenance time and costs, such as spare parts costs, and production hours [22].

IoT based applications:

Another feature IoT gives in construction technology is the IoT based applications. The use of thermal sensors and ultrasound has improved the construction process. It can assist in inspecting and taking care of the equipment according to the need. And also, by using ultrasonic sound senses the affected area [22].

Whereas, with the help of IoT technology, it saves both the cost of the production and time by determining the place and level of maintenance needed [22].

Air quality analysis:

Every nation has its laws to monitor and control air quality. Air quality analysis is the monitoring of air quality. The primary purpose of doing so is to protect the environment and people from

pollution. The quality of air influences productivity. The employee's health condition depends on the quality of the environment, thereby impacting the quality of the work [22].

However, air quality can be monitored and measured using IoT devices as well as the carbon particles, and toxic contaminants can be easily measured. Therefore, IoT does monitor health conditions and productivity [22].

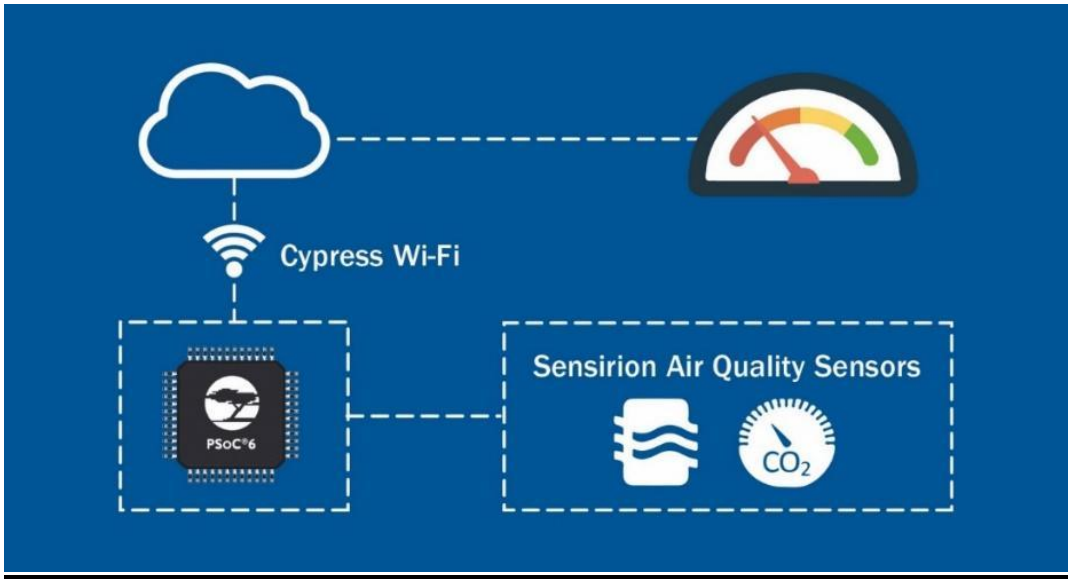


Figure 46. Air quality analysis

Source: https://www.digikey.com/-/media/Images/Product%20Highlights/C/Cypress%20Semiconductor%20Corp/Next%20Gen%20Smart%20Air%20Quality%20Monitoring/cypress-sensirion-next-gen-smart-air-quality-monitoring-large.jpg?la=en&ts=3512b76f-fa0f-4dd6-af37-18d66d280e08

Analyze and verifying with IoT devices:

IoT devices have overcome the manager's limitations. The internet of things performs equipment verification and measurement. Because of this, it has become easier to take care of the inaccessible parts, and with the help of sensors, it captures real-time data [22].

Real-time data accessibility:

In the field of smart buildings, information is a primary concern, and with the internet of things, the real-time data is now accessible. The sensors collect all the essential data and then take appropriate action accordingly [22].

IoT based green building:

Construction work is doing damage to the environment. Where IoT equipment enables the building to be eco friendly, and the buildings use the least energy. It also identifies degradation in advance. Hence, it enables appropriate action to be taken when needed [22].

IoT building components:

IoT technology takes advantage of prefabricated building components. That ensures faster and cost-effective construction. Such smart buildings often decrease the quantity of waste produced during development. Hence it offers different ways to use technology to reduce waste [22].

IoT with effective construction management:

Using IoT reduces manufacturing costs and saves time. It effectively monitors the issues and provides the most appropriate solution accordingly. The construction scenario will feature GPS tracking devices, smart inventory management, and sensor monitoring [22].

It is merely an intelligent way to manage construction work. Besides, IoT is reducing the cost of management and offering greater efficiency [22].

Energy efficiency:

Power consumption affects production costs and pollution. IoT infrastructure in building eliminates both. Some examples include temperature control sensors, actuators, energy automation with real-time communication [22].

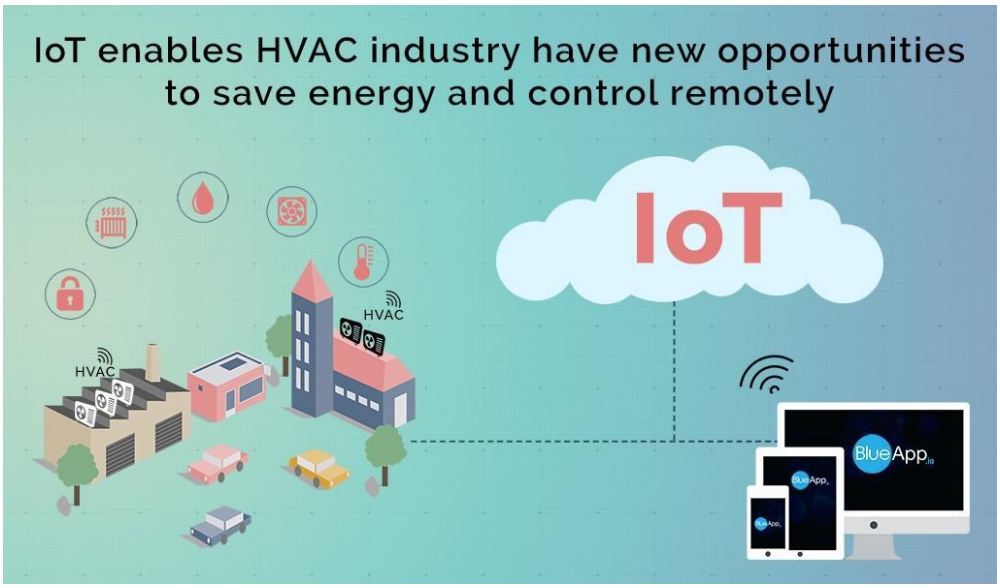


Figure 47. Energy efficiency with real-time communication

Source: https://wncgreenbuilding.com/wp-content/uploads/2018/07/IoT-for-energy-efficiency-768x449.jpg

Asset optimization by IoT:

IoT helps to manage inventories and optimize the assets. It manages big data and considers all factors. Thus, it reduces assets and energy wastage. It saves human labor as well and protects human resources [22].

The internet is the sole thing today. We rely on the Internet for everything. Proper internet usage lessens waste and increases productivity. The best example of this is utilizing IoT in smart buildings [22].

2.1 Difference between IoT Smart Buildings with and without integration

2.1.1 Smart Building with integration

The smart building or Automated buildings without integration has five distinct portions to control the entire building. All five parts, such as the fire management system, lighting control system, HVAC control system, door access, intrusion detection, and central power distribution system, are managed independently.

There is no connection among these systems. It is locally using the computer as an interface to control the building. There is no communication with humans as a network managed separately and locally. In emergencies, one system cannot transfer the signal to the other device to respond. There is no integration necessary to communicate the device with each other [24].

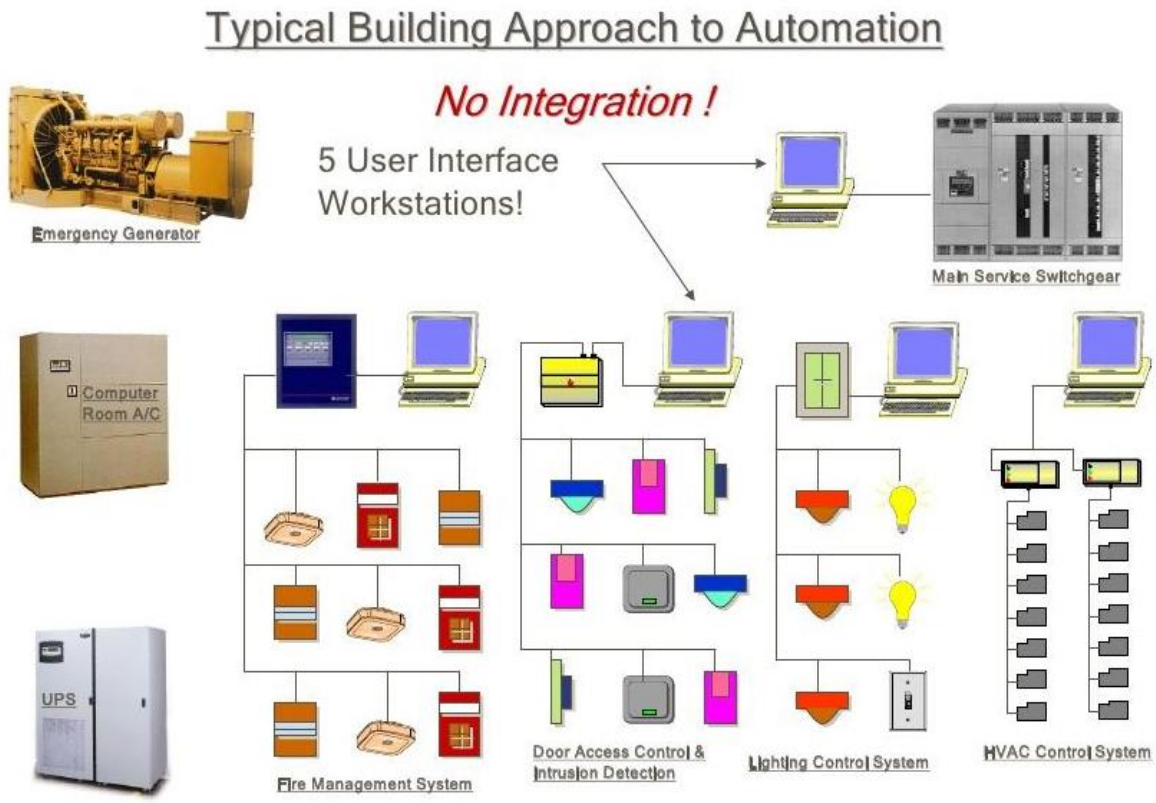


Figure 48. Smart Building with no integration

Source: https://image.slidesharecdn.com/fed-lcc-2010-greenbuildings-100615173103-phpapp02/95/fed-lcc2010green-buildings-49-1024.jpg?cb=1276623165

2.1.2 Smart Building without integration

All devices are linked to communicate with one another on a common platform. Ultimately, the entire system has one graphical user interface to manage, monitor, and feedback. The end-user can interact with the device, whether a tenant or operator. End-user communicates with the device, and the system reacts to the request of the end-user [24]. Also, in case of an emergency such as fire, all these devices respond to each other and react accordingly.

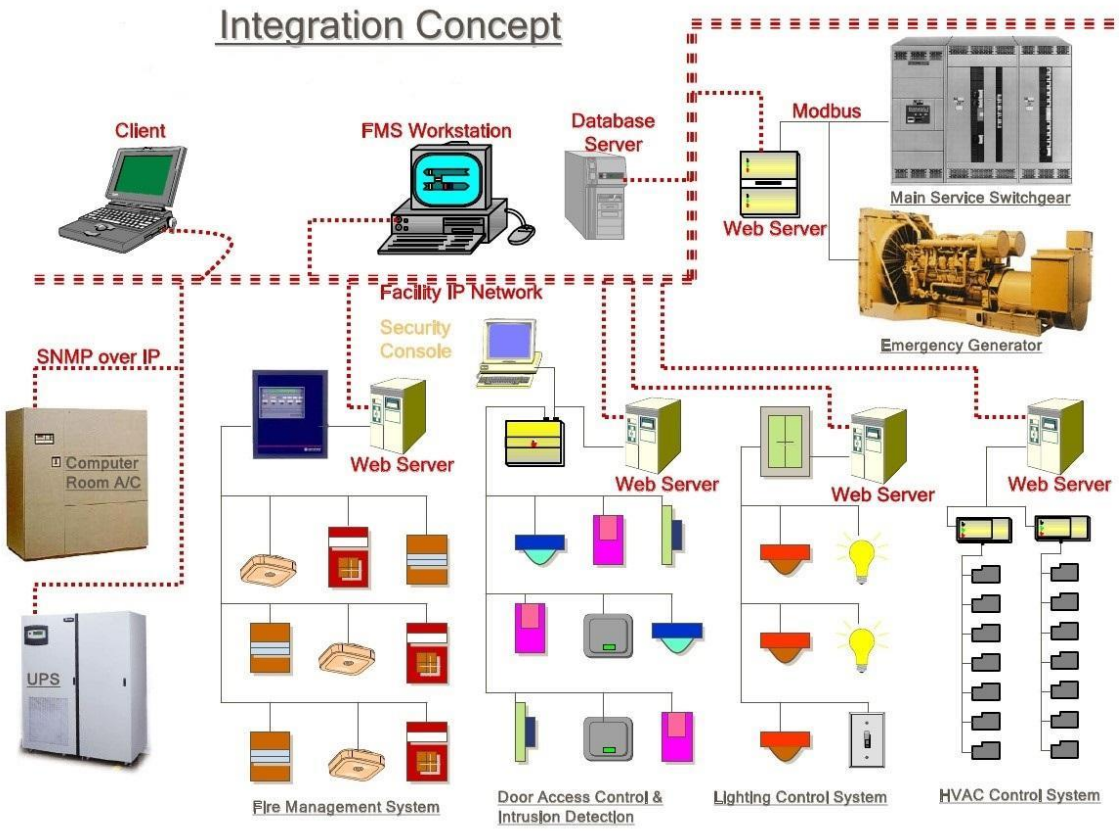


Figure 49. Smart building with integration

Source: https://image.slidesharecdn.com/fed-lcc-2010-greenbuildings-100615173103-phpapp02/95/fed-lcc2010green-buildings-49-1024.jpg?cb=1276623165

2.2 Components of smart buildings

There are five key components of smart buildings:

1. Wireless connection:

Wireless Connection plays a vital role in smart buildings as it will not be smart until it connects to the internet. Fiber still reigns, and this stays a fantastic convenience that no building owner would want to stop without contemplating their construction project [25].

2. Smart light:

It is one of the latest developments in the lighting business to improve the efficiency of lighting. The wireless intelligent nodes are at the core of any intelligent lighting project. These modules generate a mesh network to which we can link sensors like air quality building protection and many more [25].

LED lighting retrofits are rising in demand as the building owners search for energy savings methods. The connection of these LED luminaires allows for the ideal IoT infrastructure [26].

Connected, intelligent buildings provide intelligent workspaces that encourage higher productivity and can also save energy and reduce waste. Smart buildings need a firm data-carrying communication infrastructure; that is where smart lighting takes the lead [26].

Whereas, wireless technology is used by building engineers to link the luminaires in new and existing structures. For instance, the Zigbee lighting-specific wireless control platform is used to support an IoT control system, and it should be able to receive all forms of data traffic [26].

Hence, it is safe to state that they play a crucial role in the creation of energy-efficient power systems for use in residences, businesses, industrial infrastructures, and smart cities [25].

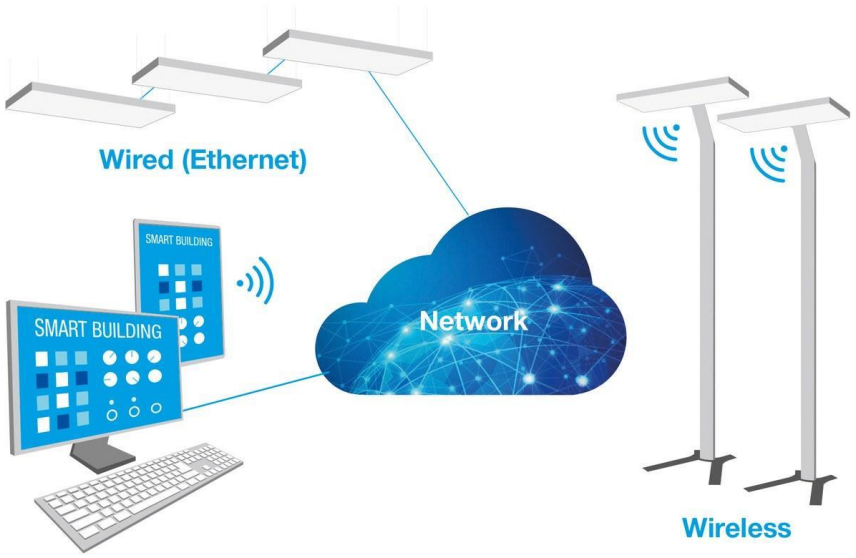


Figure 50. Smart light

Source: https://www.led-professional.com/technology/electronics/the-201cinternet-of-light201d-2013-the-key-to-the-201cinternet-of-things201d/@@images/52ea9f14-7ead-4ea0-80be-1daf9537cfdf.jpeg

3. Security:

As a tech-savvy building owner, the project is not complete until it has been able to succeed in taking the benefits of a network-based security system. It can begin with the deployment of CCTVs for security monitoring. However, now it can be so much more. Link the surveillance system to the internet, and they can be remotely controlled and hooked up to software for image analysis. Imagine being able to track the property from miles away and everything that is going on within the building, without any physical presence needed [25].

Figure 51. IoT based security camera

Source: https://www.swann.com/blog/wp-content/uploads/2018/06/IMG_9171_intcam_battery_cam_in_situ_lifestyle_outdoors_wall_bush_exposed_weather-e1530050345741.jpg

4. Advanced HVAC systems:

Smart Buildings now have an advanced HVAC system that will be installed during the construction phase. This mechanism can be managed with an app or software, which is possible because of wireless technology [25].

Moreover, some of these advanced software and apps can also be utilized to monitor the HVAC system's water flows, fan speeds, and pump speeds, all done to maintain pre-specified temperatures. In other terms, if you have this kind of approach, building residents don't have to experience unnecessary cooling or heating [25].

Advanced heating, ventilation, and air-conditioning (HVAC) systems may reduce consumption in an empty area of a building. It can also adjust the process, continue to match demand, and predict maintenance requirements. These are focused on sensors and use control strategies that are adapted to the system technologies through modulating temperatures, flow rates, capacity, and more [27]

5. Reduce energy consumption:

The energy management system, linked with smart meters, allows building tenants to program how and when they want to use their energy. These technologies are promising to reduce the costs of electricity and make better use of what the occupants already use. For example, when there is a higher demand for electricity, the device may limit the use of excessive power at peak hours. Also, to put it another way, the system allows shifting the bulk of power use to off-peak periods [25].

2.3 What makes smart buildings "smart"?

Intelligent buildings are basically buildings with a mind, and that "mind" is a building automation system. Which monitors and controls all of the functionality of a building from a single management hub. Heating, cooling, air conditioning (HVAC), lighting, and other factors for life safety controlled by building automation systems [33].

Advanced BAS technology implements buildings to operate at a much higher capacity than before. There are four most important components of building automation systems technology that converts bricks and concrete into smart buildings, which are as follow [33]:

1. Advanced monitoring:

Earlier technology would employ a single sensor to monitor the environment of a whole floor. According to Cisco, recent technologies include "smart dust, micro-sensors, and wireless mesh communications" now allow for control of every single piece of equipment in a house. Building

automation systems have an accurate picture of the building efficiency, with thousands of sensors continuously collecting data [33].

2. Cloud-based management:

In comparison to building automation systems from years ago, today's systems store information regarding building and managing operations in the cloud [33].

As per real estate experts at Jones Lang LaSalle, with the "high-capacity cloud computing technology" controlling operations, BAS will gather a more significant amount of data, and thereby handle building performance much more effectively. Centralizing services in the cloud often ensure that the performance of a building can be managed at any time, anywhere [33].

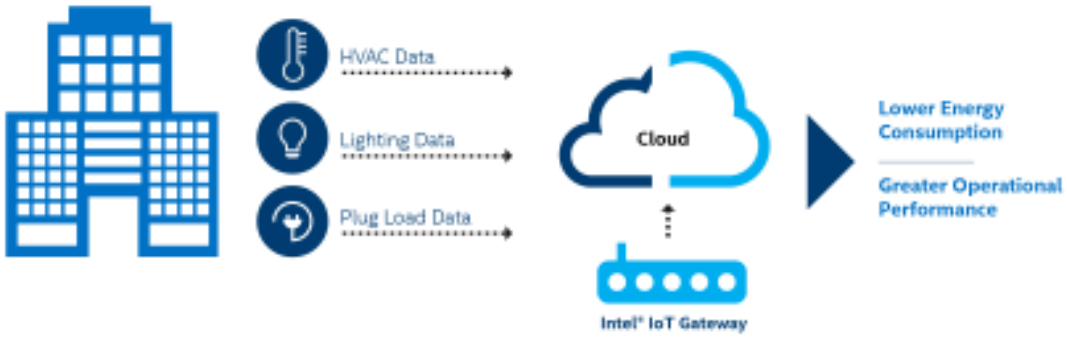


Figure 52. Cloud-based management in IoT smart building

Source:https://www.intel.com/content/dam/www/public/us/en/images/illustrations/smart-building-affordable-energy-management.png.rendition.intel.web.480.270.png

3. Machine to machine communication (M2M):

Advanced BAS technology integrates the multiple systems in the building. Apart from having independent control of heating, ventilation lighting respectively, new technology connects these functions and makes them interoperable. With the help of interoperability, it provides intercommunication. All of these devices will effectively "speak" to each other, thereby allowing maximum effectiveness. Wasteful conflicts with the device, such as cold and hot air blowing

concurrently, can be prevented. Smart technology today also allows for communication between separate buildings as well [33].

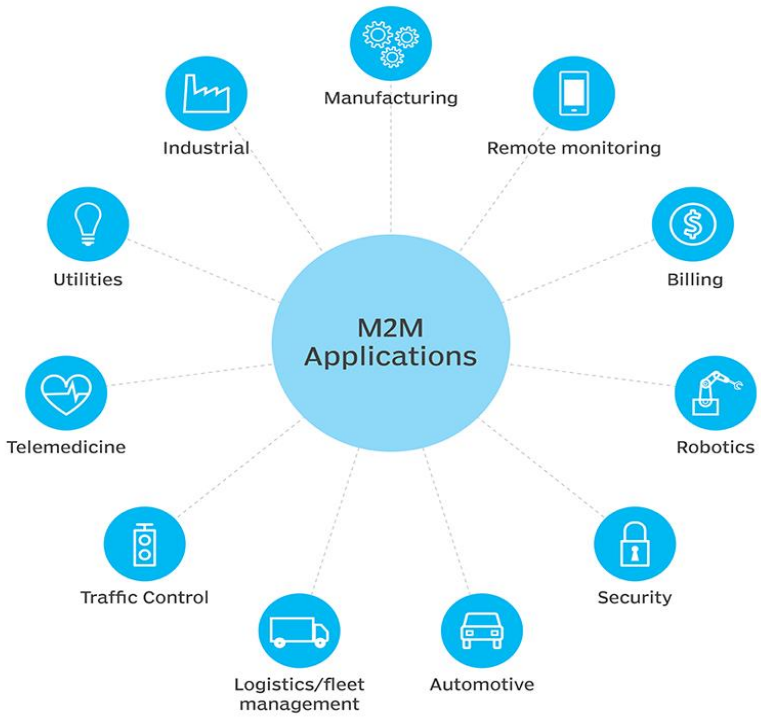


Figure 53. M2M communications

https://cdn.ttgtmedia.com/rms/onlineimages/iota-m2m_apps.png

4. Continual commissioning:

Conventional buildings need to regularly recalibrate their facilities, such as lighting ventilation, air conditioning, respectively. Latest building automation systems practice "continuous commission," which obsoletes such periodic check-in. The precise control and intelligent maintenance that BAS allows ensures that buildings can adjust the machinery in real-time. They continuously collect data from the system and adjust the energy usage accordingly. Consequently, "a smart building system guarantees optimal performance all the time and eliminates waste much more efficiently than a periodic process can match [33].

2.4 Non-energy benefits of smart building

If smart technologies are to flourish in the market, the building industry needs to understand the value proposition of intelligent buildings better and start shifting the culture of building operators [31].

This study intends to explain how smart buildings can save energy. But for non-energy purposes, many building owners are retrofitting smart steps into their premises. The 2016 Energy Efficiency Indicator Survey asked more than 1,200 executives in facilities management on essential drivers for investment in their buildings in energy efficiency. Two-thirds suggested that significant investment drivers were the growth of their company brand reputation and the attraction of new tenants [31].

Business owners also realize the benefits that investment in energy efficiency has for employee well-being and productivity. One study found that a 2 percent improvement in employee productivity amounts to save operating costs of $6 per square foot [31].

Smart buildings add value to lease and sales, and business owners are starting to realize this. While consumer awareness of energy efficiency continues to expand, and energy performance data construction is becoming readily accessible, potential renters and owners will make better choices regarding leasing or purchasing buildings based on energy usage and related energy costs. Smart building owners can also fulfill growing customer expectations regarding flexible workspaces and autonomous operation [31].

Also, this growing demand from occupants for energy-efficient and scalable workspaces will lead to increased market adoption of smart design technologies [31].

The smart buildings also have other advantages. Devices operating over wireless Internet networks can be easier to install and do not compete with current building finishes. In addition, to manage primary energy-consuming systems, smart buildings also incorporate security, access, and safety systems management in the building. Building owners can use reasonable steps to both improve remote controllability of their buildings and assess efficiency across their portfolio [31].

Furthermore, several smart buildings generate power on-site by distributed generation systems and engage in demand response activities to mitigate peak energy use of the building to help stabilize the power grid [31].

2.5 Existing smart building technologies

Maybe no technology trend has had a more significant influence on facility management than investing in "smart" building technologies. This multi-billion-dollar market is growing leaps and bounds, emphasizing technology that varies from automated climate control to smart parking garages to self-cleaning restrooms, as well as many other known and unknown use cases [28].

Furthermore, some common smart building technologies tend to overlap or communicate often with each other, and it is essential to distinguish them separately, as each offers a distinct layer of functionality. In the following section, some of the technologies will be explained briefly [28]:

Internet of Things (IoT)

The internet of things is the most critical and popular smart building technology. It uses a standard Internet Protocol (IP) interface to connect multiple devices, including sensors and microchips, to share and analyze the data while automatically improving the functions of each device. Whereas, when aggregated across a whole building, then IoT enables the digitization of assets throughout the facility, and therefore it leads to rapid improvements in efficiency [28].

In the smart home use cases, which are as self-learning thermostat and intelligent utility meters, the IoT has become most popular. Moreover, various technologies have recently emerged within commercial and industrial environments, both internal optimizing operations (for example, IoT-enabled Asset Condition Management) and enhancing the resident experience [28].

In many cases, IoT-enabled devices are controlled and connected via a mobile app over the internet, providing those who use them a convenient and user-friendly experience [28].

Toilets with a Smart toilet system are one of the effective uses of IoT in industrial facilities. As the quality and cleanliness of the washrooms typically cause the majority of complaints from occupants and push customers away quickly. Even before the issue arises, IoT sensors solve

problems like smart soap and paper towel dispensers, for instance, automatically warn cleaning crews when the levels are low, or even self-restock if required [28].

Smart occupancy trackers decide when a toilet is full and let visitors find out about its estimated waiting time via a mobile app. This sort of sensor often schedules cleaning teams on the back end after a specified number of visitors have gone to the washroom [28].

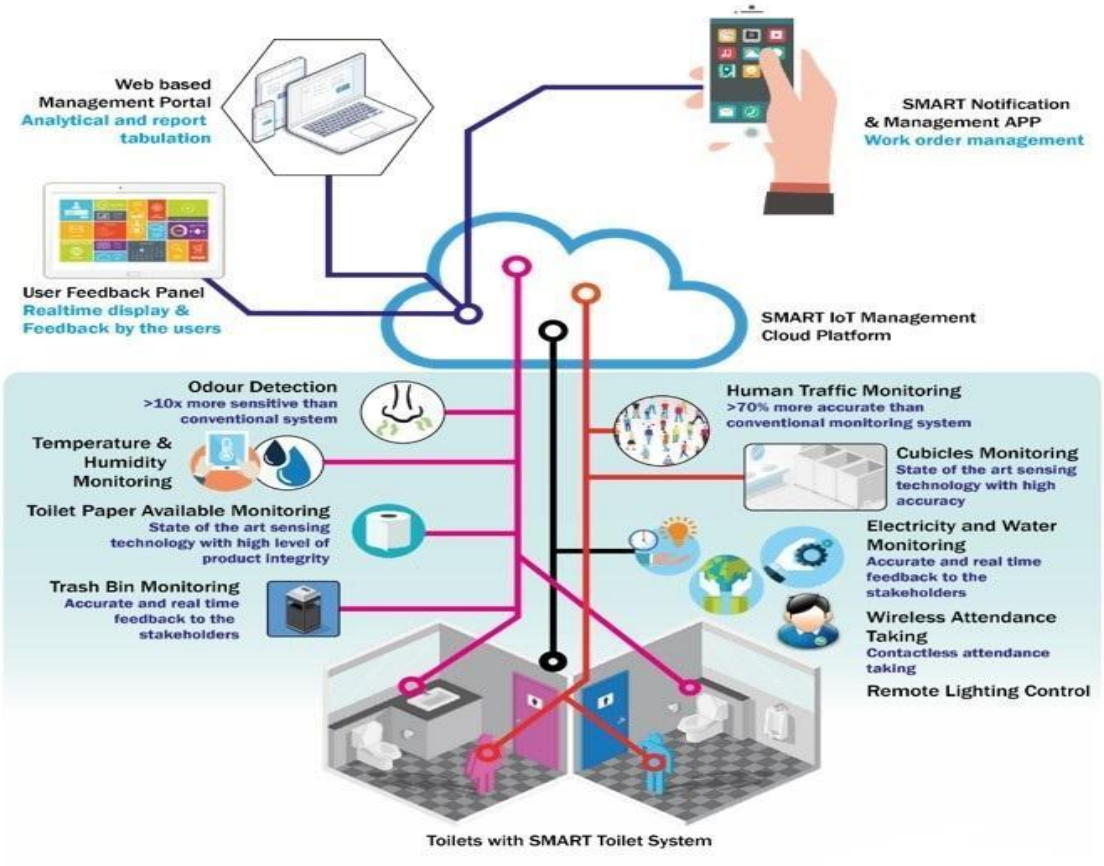


Figure 54. IoT Based smart restrooms in smart building

Source:

https://inno.emsd.gov.hk/filemanager/itsolutions/common/upload/6/192/Smart%20Toilet%20Theme.jpg

Machine Learning and Artificial Intelligence

Like IoT, Artificial Intelligence (AI) is a phrase that has been gaining quite a bit of attention nowadays yet is often misunderstood. Artificial Intelligence is the process through which machines or software imitate human behavior and intelligence, with the ability to acquire knowledge and apply it. It supports optimization basically, decision-making, without human interference within the machine or software [28].

Machine learning (ML), frequently mistaken as a synonym for AI, though it is a technique for understanding AI. It refers to the process through which a machine obtains knowledge or skill. In smart buildings, AI applications are extensive, particularly as AI is easily integrated with IoT sensors and devices. These devices introduce fundamental thinking to understand objects and situations hierarchically as well as make changes to user preferences observed or analyzing historical trends [28].

For example, an asset management system enabled by AI and IoT can pick up on irregularities in equipment operation such as a leaking refrigerator based on what it has "learned" about the machine's energy input or output when it usually runs. Also, the AI-enabled Service Automation program predicts future repairs and even feedback and approves work orders with minimal human interaction [28].

Building automation

Building Automation is a comprehensive infrastructure that permits centralized control of the HVAC, lighting, security, and other systems of a building. Building Automation is managed by either the Building Management System (BMS) or the Building Automation System (BAS) which is a central digital or mobile hub. These systems are also compatible with IoT solutions and can monitor and control essential factors such as temperature, humidity, electricity, water pressure, and many more [28].

Building Automation's advantages include increased energy efficiency, decreased operating costs, and increased occupant comfort through a centralized network and carefully aligned controls [28].

For example, a Building Automation System could be designed to turn up the air conditioning and improve airflow in a specific conference room when it detects that someone switches on the lights of the conference room. It even works in conjunction with AI and IoT systems, such as learning that this conference room will be used from 10:00 a.m. -11:00 a.m. Every Tuesday and then a few minutes before adjusting its climatic settings [28].

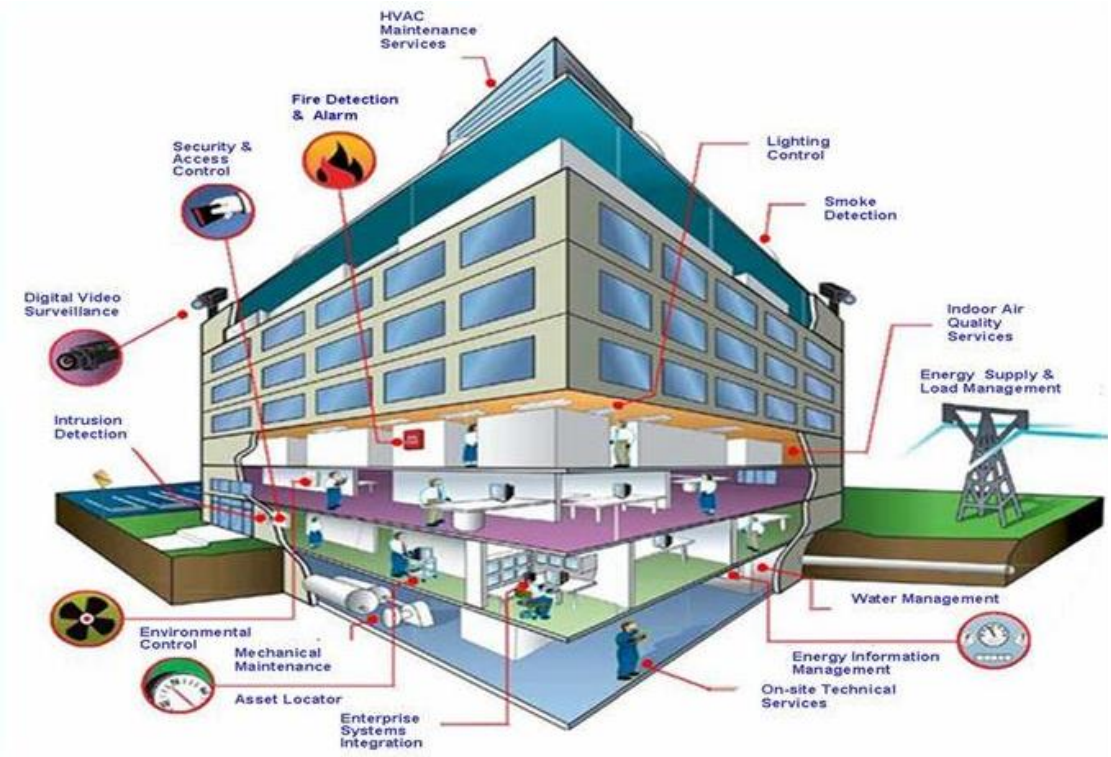


Figure 55. Building Automation System

Source: http://sauhperkasa.com/wp-content/uploads/2019/02/03-BAS-Ilustration-source-Techiexpert.com_.jpg

Cloud computing

Cloud computing offers virtualized platforms with flexible compute and storage capacities. Cloud platforms are generally run as a service based on big data centers and enable additional computational (that is CPUs) and storage capacity (that is disc space) when needed. It can eliminate a software-based enterprise's need to gain and maintain its computing infrastructure.

Flying drones

Drones are not only valuable for taking aerial photographs or delivering packages, but they can also be used to provide intelligent support within a building or retail space. It can take on many routine or time-consuming tasks and free up employees to focus on more important things. Defined as an "unmanned aerial vehicle," drones are controlled remotely, and may also use AI for autonomous operation [28].

Drones conduct a wide variety of tasks that benefit their operators for smart office space, retail facility, or even a grocery store: by searching shelves for expired products to check hard-to-reach devices such as rooftop machines to identifying intruders in an office building, they act as an additional set of simply maneuverable "eyes" that sense minute details and work at all hours of the day. Moreover, it can also help during construction in a smart building. However, drones are affordable, agile, and relatively easy to deploy [28].

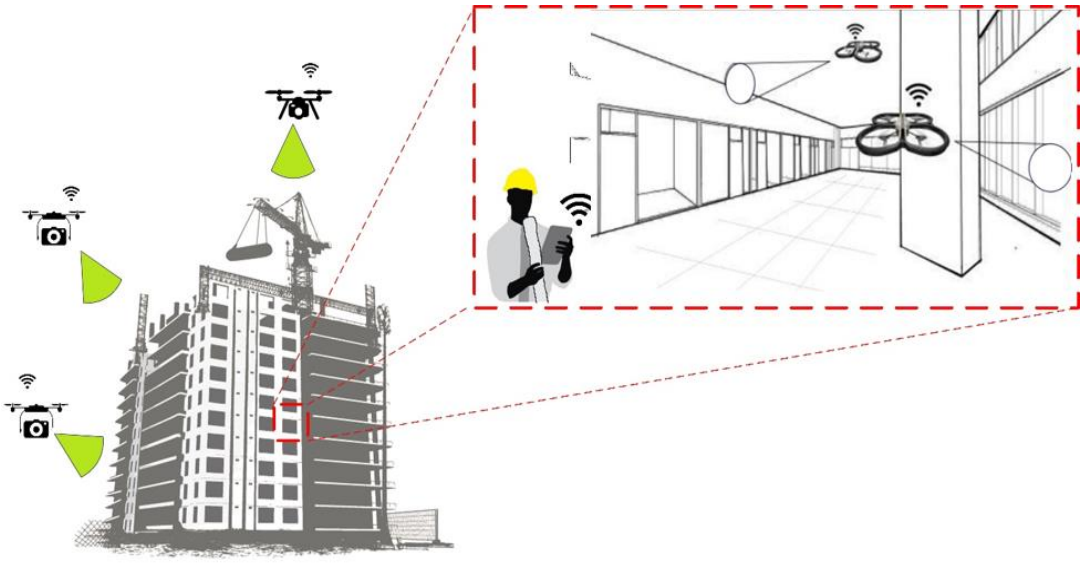


Figure 56. Flying Drones in Smart Building

Source:https://civmin.utoronto.ca/wp-content/uploads/2017/05/figure-1-hesam.png

Building Information Modeling (BIM):

Building Information Modeling (BIM) is a smart 3D model-based method that records and displays a facility's physical and functional characteristics. Historically, AEC (architecture, engineering, and construction) professionals used BIM mainly, but it has increasingly become more prevalent within the context of facilities management [28].

A highly practical tool for both building maintenance and continuing use, BIM acts as a building handbook" of sorts that provides access to real-time asset profiles as well as increased knowledge of asset locations [28].

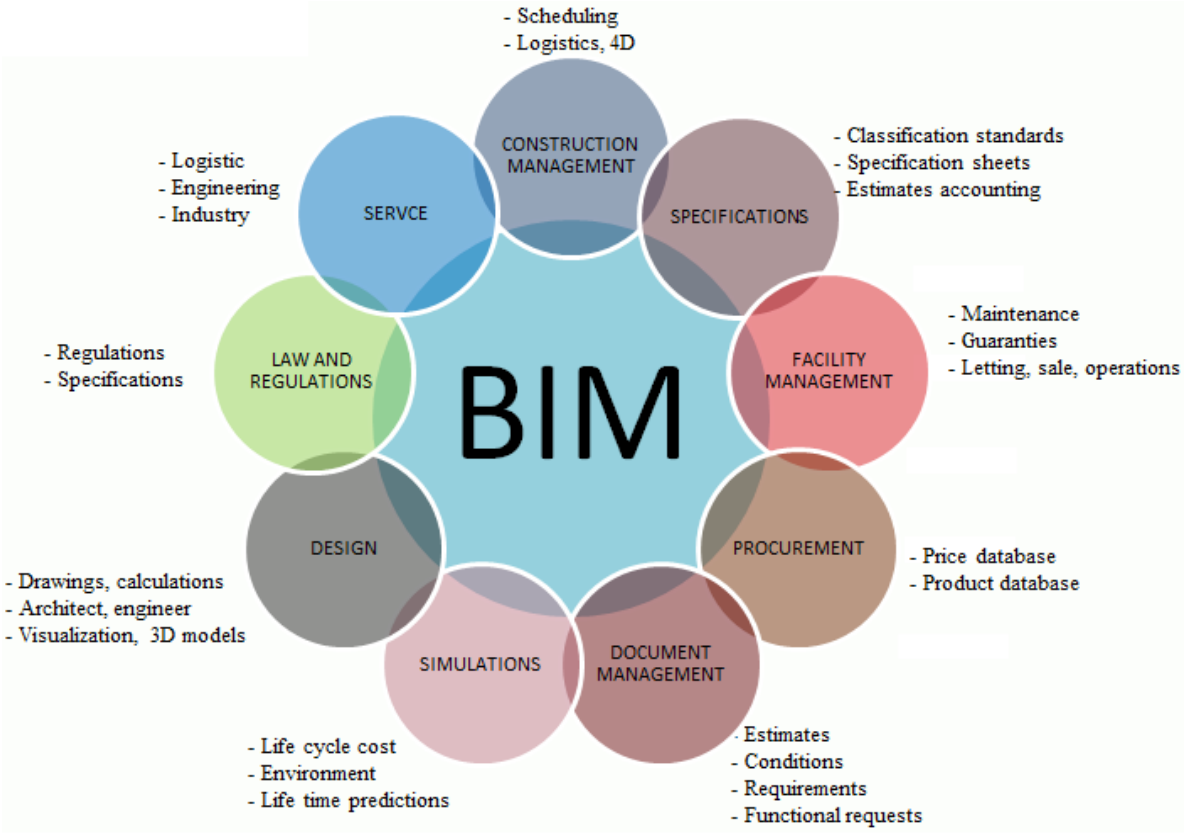


Figure 57. Building Information Modeling

Source:

https://www.researchgate.net/profile/Lukasz_Nazarko/publication/323401191/figure/fig1/AS:598349925318682@1519669147818/Building-Information-Modeling-BIM-lifecycle-view-17.png

For example, where precisely a specific electrical circuit or equipment component is located behind a wall. Beyond geographic knowledge, it offers insights into the spatial knowledge, light analysis, and building component quantities and properties [28].

This kind of visual and spatial knowledge is astonishingly useful when restoring or renovating buildings. Using BIM software, one can ultimately "grab" and move a wall object around to determine whether it could be placed somewhere else. This process shows possibilities for better space utilization and enhanced building efficiency. Additionally, BIM allows endless test situations without ever having to touch the space physically, which means reduced downtime and reduced labor spending [28].

Augmented Reality (AR):

Augmented Reality (AR) is a live, copied view of a real-world environment with computer-generated sensory input complementing its elements. Basically, it requires a camera and some display device like a laptop, smartphone, or even eyeglasses, expanded reality superimposes an imaginary object onto a view of one's actual, physical environment [28].

The AR technology is particularly helpful for facility management when it is used in combination with BIM, for example, slipping on a pair of AR-enabled glasses (such as the Microsoft HoloLens) while inspecting a plant room filled with various unknown electrical and mechanical devices. Programmed with current BIM models, the glasses allow to display "hovering" digital representations over each piece of equipment, offering recognition and additional information. Such knowledge may include written instructions, alerts, installation dates, and problem-solving, all of which are particularly useful during outages or emergencies [28].

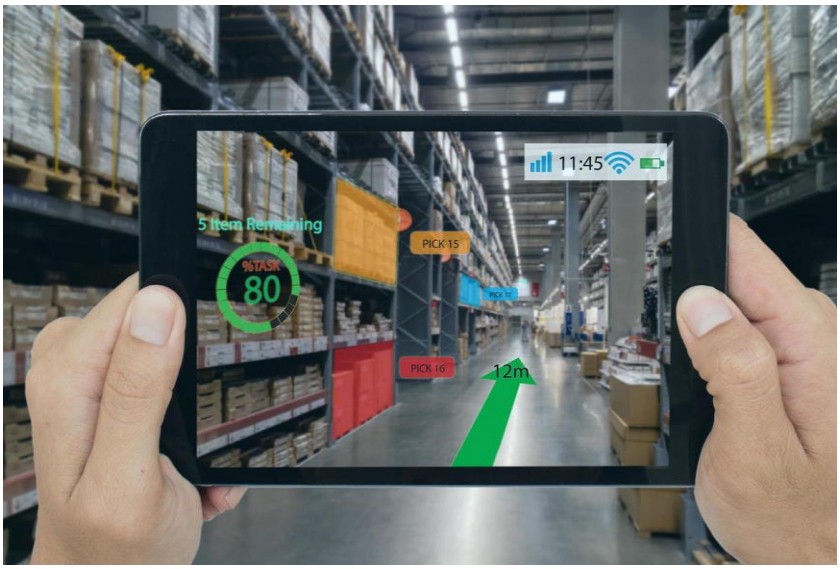


Figure 58. Augmented Reality in smart building

Source: https://tr1.cbsistatic.com/hub/i/r/2019/12/16/4ff17863-74c6-425a-be4a-42e245fd272f/resize/1200x/d63ead87cc8b3f586acb3cb42022456c/istock-1126094461.jpg

Virtual Reality:

Virtual reality (VR) goes a stage further with computer-generated sensor input providing a full immersion experience by blocking out the physical world and turning the user into a realistic, virtual environment. Whereas, the design and construction industries have adopted VR as a useful tool during the mockup phase [28].

VR-powered mockups enable a customer to view a potential building as if visiting the space where the customer may walk around, inspect windows and staircases, and get a sense of the constructed structure's layout and function before any work has begun [28].

While virtual reality within the facility management industry is still far from widespread, the technology has started to become more powerful and affordable in recent years. The potential benefits of VR are dynamic quality checks, internal 3D design analysis, and even virtual walkthroughs using VR devices are all made possible [28].

VR data can also be integrated into applications for facilities management and used for repair and upkeep. Many start-ups have already started exploring VR in the FM context. For example, New

York-based Iris VR provides two solutions, which are desktop software and mobile apps that integrate 3D BIM models into VR to provide a 1:1 scale collaboration and design analysis platform. Hence, these technologies are making a smart building more effective as well as cost-effective [28].

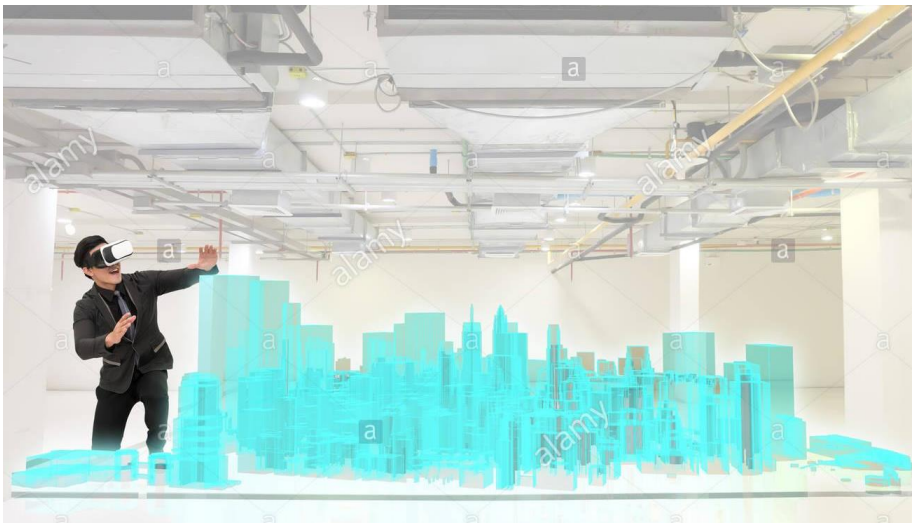


Figure 59. Virtual reality

Source: https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcT4Seye9J1XB8DUxXyoKvLb11D5AR2jDcNNt7udfu63XdspNn2a

2.5.1 Examples of smart buildings

Smart buildings are becoming increasingly popular and represent the future of construction and real estate. It could relate to complex organisms whose network has interlinked, and this is possible because of modern information technology, which intends to make them more active. Soon they will integrate technologies that will go beyond automated lighting or even HVAC network configuration such as Heating, Ventilation, and Air Conditioning [29].

In fact, they are destined for bigger things, such as advanced real-time energy efficiency control, or comfort and access optimization, and many more. Moreover, to achieve this, the integrated networks are linked to different building elements, sometimes in different ways, and sometimes by systems that are not fundamentally physical [29].

In the case of highly advanced smart buildings, the devices with which the building is equipped are linked via an external network (such as the Internet) and, therefore, can be remotely controlled. Most of the cutting-edge approaches in smart architecture lack some architectural credibility but still demonstrate effectively how digital conception may affect the economic, structural, or energy profile of a building [29].

To illustrate these different aspects, some examples of current smart buildings have been chosen and briefly explain in the following sections:

1. NASA base in Moffett Field, California, for sustainable development

This crescent-shaped building boasts smart control technology influenced by the agency's air safety program, which provides air flight controls, most prominently. This technology is used to monitor multiple building zones and to provide real-time data on the flows through the structure. Whereas known for its unique approach to permanent recycling technologies, William McDonough Partners used renewable, recyclable, or recycled materials in the design of the building. Furthermore, within this building, many other devices and technologies have been implemented to optimize its energy aspect [29].

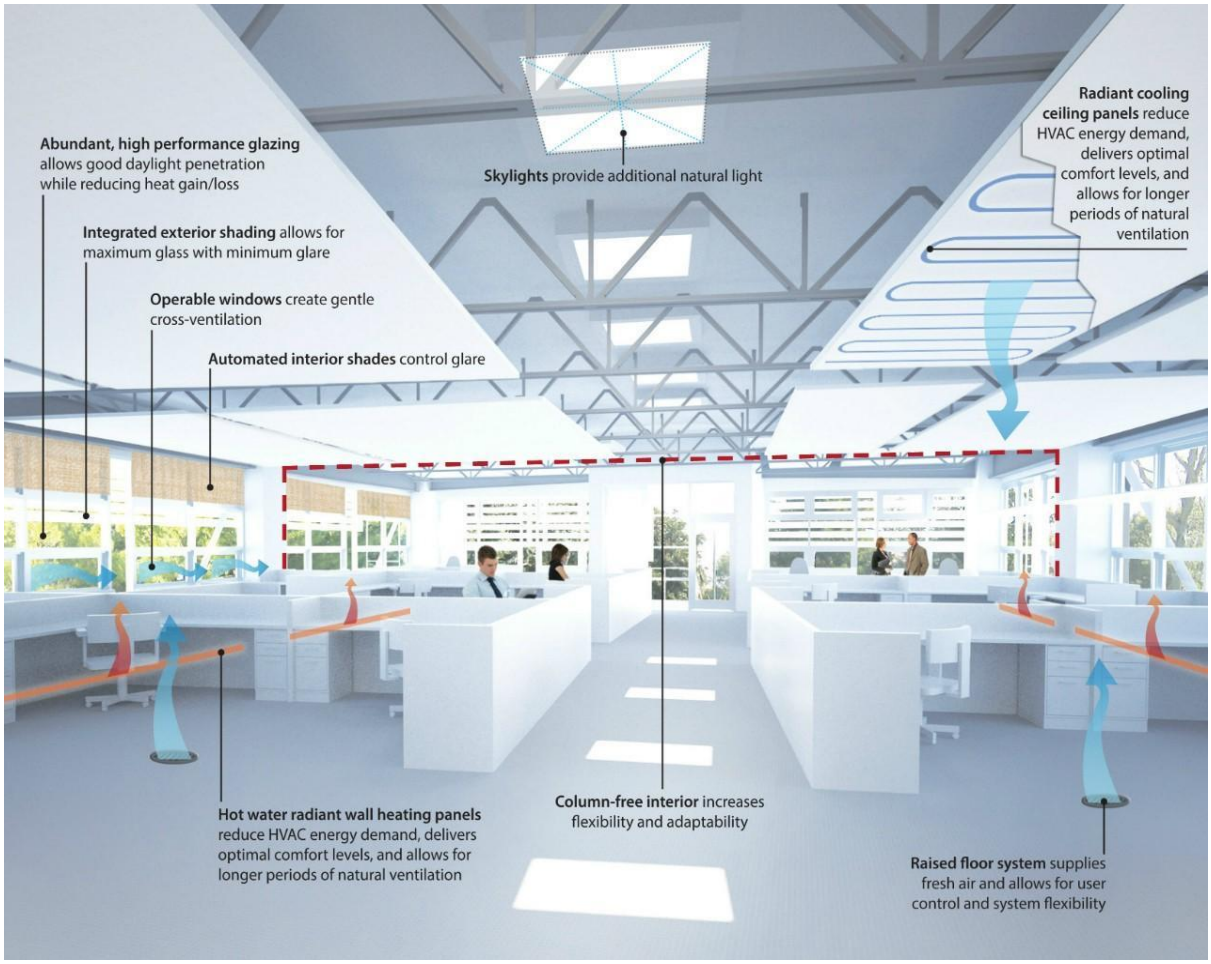


Figure 60. NASA sustainable development base

Source: https://d2gs61btqzt6ta.cloudfront.net/blog-news-photo/a2-81-fb-90-29-4b-93-0d-f4-59-37-b7-a1-a3-ad-c9-8e-95-29-05.jg .

2. Burj Khalifa, Dubai

Dubai is a world leader in the smart building trend. Also, "Honeywell" gave a score of 65 out of 100 to this country's smart buildings. This score evaluates the sustainability, security, and productivity of the buildings [2].

Whereas, the Burj Khalifa already had the remarkable reputation of being the world's tallest building with 160 floors, standing at 2,716 feet tall [2].

However, now with Honeywell's support, it is one of the smartest and most sustainable buildings. Honeywell partnered with building managers to introduce many smart building projects at its

marquee location, which increased air quality, lighting, and temperature for its occupants. The building automation network transmits real-time information to Honeywell's IoT platform and utilizes advanced algorithms to detect irregularities and maintenance issues. Moreover, facility managers may employ this information to enhance building maintenance and asset reliability [2].

Figure 61. The Burj Khalifa, Dubai

Source:

https://www.google.ca/search?q=burj+khalifa+best+picture&tbm=isch&ved=2ahUKEwjOwe6hjMjnAhVe9qwKHRNhDbsQ2-cCegQIABAA&oq=burj+khalifa+best+&gs_l=img.1.2.0l7j0i8i30l3.126628.128022..129820...0.

0..0.106.571.4j2.....0....1..gws-wiz-img.CAiVg8vIBlE&ei=kuFBXs6wNt7sswWTwrXYCw&bih=332&biw=767#imgrc=GzCaGuJEjx0HM

3. Algenhaus:

Hamburg is home to the world's first building equipped with a full front of bioreactors. Positively filled with innovations, this building features an exterior that is both insulating and generating energy. In reality, algae are actually produced in it, which creates biogas, and it can be utilized for heating purposes or as fuel. It can also be saved and transformed to be turned into electricity or heat by a generator. Moreover, biogas can be used in many other ways [29].

The working process is as follows: firstly, the algae suspends in a thin sheet of water held by two layers of glass and is continuously fed by a water circuit containing nutrient and carbon dioxide. Secondly, the algae photosynthesize and multiply in a regular cycle by using the sunlight. When collected, isolated, and transported in a thick pulp (biomass) to a technical chamber, then it is used to produce the biogas (methane) [29].

Figure 62. Algenhaus (Hamburg)

Source: https://d2gs61btqzt6ta.cloudfront.net/blog-news-photo/a2-81-fb-90-29-4b-93-0d-f4-59-37-b7-a1-a3-ad-c9-8e-95-29-05.jpg

4. World Trade Center (Bahrain)

The World Trade Center located in Manama, Bahrain, is a modern take on traditional wind turbine towers, most notably used to harness offshore winds in the Arab Gulf [29].

This smart building's shape channels the airflow through three turbines, each with a diameter of 3 meters. It is supported by walkways linking the two 240 m towers. The turbines produce about 11 to 15 percent of the energy needs of the buildings [29].

It is designed by the architect Atkins, and the Bahrain WTC has won several awards for organizing renewable energy into its large-scale infrastructure design, including the 2009 NOVA Award for integrating technology to enhance sustainability and reduce development costs [30].

Figure 63. Bahrain World Trade Center

Source: https://d2gs61btqzt6ta.cloudfront.net/blog-news-photo/a2-81-fb-90-29-4b-93-0d-f4-59-37-b7-a1-a3-ad-c9-8e-95-29-05.jpg

5. ZCB mansion, Hong Kong

It is the first zero-carbon building. The ZCB mansion integrates passive design features with high energy efficiency active systems such as large-volume, low-speed HVLS fans, a chilled beam air-conditioning device, and smart control systems capable of reducing energy requirements by 25 percent. Energy production for the building is currently sufficient for its own needs, but now it is looking to go beyond carbon neutrality by producing much higher quantities of electricity [29].

The customized BEPAD (Building Environmental Performance Assessment Dashboard) system displays data in real-time. It evaluates the environmental performance of the building, providing information on general energy consumption, water use, occupancy of rooms, indoor air quality, and so many. These are managed by the BMS (Building Management System) that collects data from 2,800 detection points across the whole system [29].

Figure 64. ZCB mansion, Hong Kong.

Source: https://d2gs61btqzt6ta.cloudfront.net/blog-news-photo/a2-81-fb-90-29-4b-93-0d-f4-59-37-b7-a1-a3-ad-c9-8e-95-29-05.jpg

6. AI-Bahr, Abu Dhabi

Equipped with a dynamic shading system designed to reduce solar gain from the building by 50 percent, the Al Bahr Towers are pushing the dynamic design limits. The exterior is fitted with a system motivated by traditional Mashrabiya, but computerized to match evolving weather conditions in this case [29].

The Mashrabiya is a forced natural ventilation system which is often used in Arab countries ' traditional architecture. The surface reduction induced by the Mashrabiya latticework speeds up the wind flow. Furthermore, then the air is brought into touch with wet surfaces, basins, or dishes filled with water that spread cold air across the building's interior [29].

Figure 65. AI-Bahr, Abu Dhabi

Source: https://d2gs61btqzt6ta.cloudfront.net/blog-news-photo/a2-81-fb-90-29-4b-93-0d-f4-59-37-b7-a1-a3-ad-c9-8e-95-29-05.jpg

7. The Crystal building, London

The Crystal Building is the world's largest permanent exhibit site dedicated to the study and creation of sustainable cities, and one of the world's most sustainable buildings. It is in London, England [32]. It provides so many features, such as:

- The yearly heating bill is Zero.
- It produces 70 percent less carbon dioxide.
- The water in its restrooms is 100 percent recycled.
- It uses 46 percent less on energy than any other building of its size.
- By using the solar panel and ground heat pumps, it generates energy.
- It saves rainwater to manage the restrooms and irrigation systems.

Figure 66. The Crystal building, London.

Source:https://www.filmoffice.co.uk/umbraco/imageGen.ashx?image=/media/219502/The-Crystal-Mordern-Glass-Architecture-53.jpg&class=locationImage

3 Security issues and challenges for the IoT based smart building

3.1 Security issues in smart building

A security risk has risen in smart buildings from the past decade. Whereas, a wide range of ways through that hackers and cybercriminals can probably attack a network via a smart building solution [34].

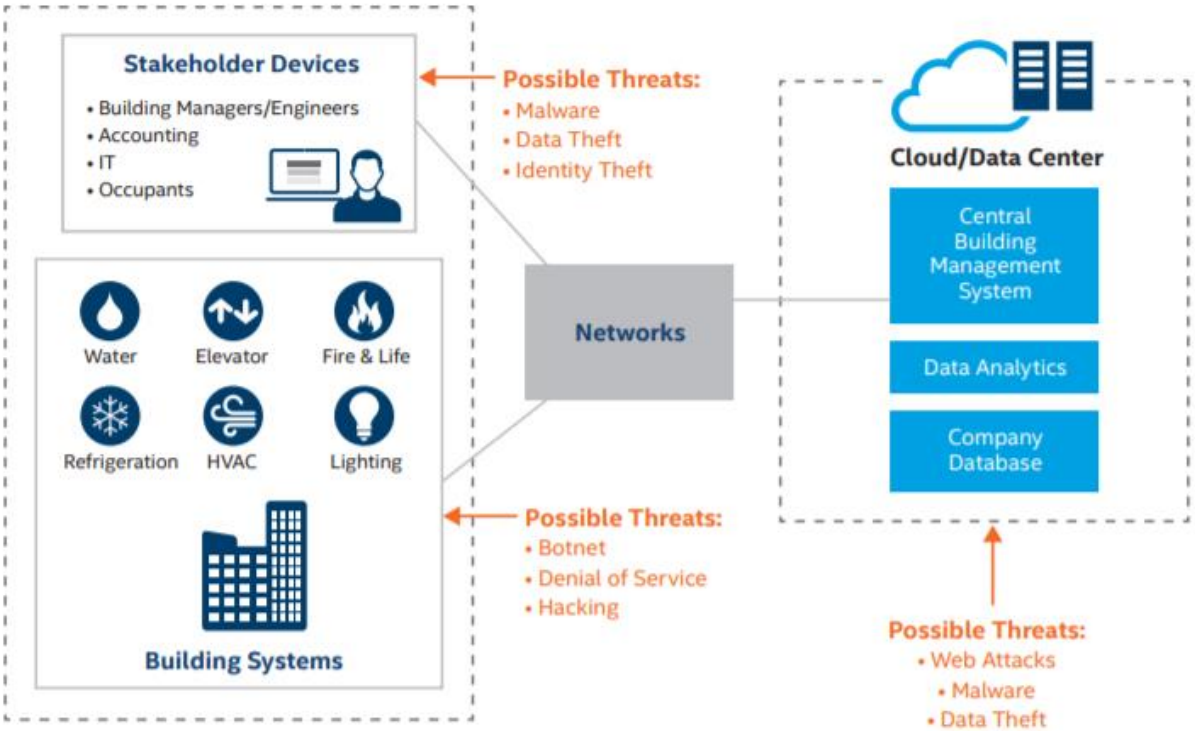


Figure 67. Security threats in IoT based smart buildings

Source: https://cdrdv2.intel.com/v1/dl/getcontent/334327

a) Security threat in the area of stakeholder devices

A smart building can connect a variety of building systems such as HVAC, lighting, cooling, and surveillance and stakeholders, which include building managers, engineers, accountants, finance, IT, and tenants. Therefore, these can be targeted by possible threats including [34].

1) Malware

As building systems do not surf the web or open emails, they still require to be protected from malware hiding in message payloads that could cause serious problems, such as attacking mission-critical data or creating damage to equipment. It is also necessary to assure that malware can not access building systems via removable storage media such as USB drives, CDs, and DVDs. Many believe the Stuxnet virus was spread in this way [34].

Additionally, personal computing devices used by customers to communicate to the building systems or the BMS through a user interface often require security protection. Due to an infected device, malware could hack the smart building [34].

Malware usually targets personal devices through websites, email attachments, executable files, and much more, creating it essential to protect all devices which link to the network, whether private or public, for example, 4 G, Internet. Many stakeholders are aware of cybersecurity risks, though the user remains the weakest link when it comes to phishing attacks. According to the 2014 report by Version Data Breach Investigation states that almost one in five customers would click on the link inside the phishing email [34].

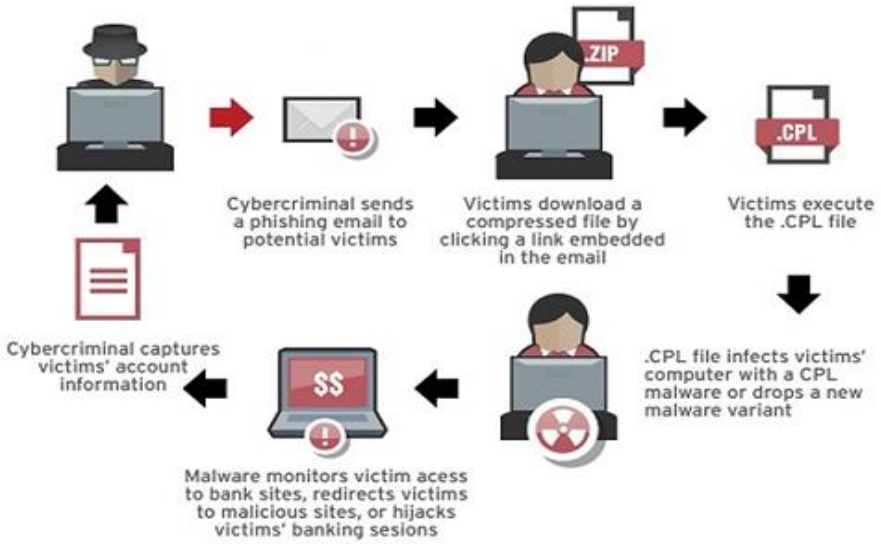


Figure 68. Malware attack

Source: http://blog.trendmicro.com/trendlabs-security-intelligence/files/2014/03/cplpart2-5.png

2) Identity theft

Individual identity theft, either internal or external to the company, may wreak havoc if they acquire privileges from the administrator that allows them to control the system in any way they wish. It often occurs through an unsuspecting user or administrator who clicks on a phishing email and gives up their login credentials. Thieves will place a virus once they get on the network, steal data, control the system, eavesdrop on data being sent, or a plethora of other evil offenses. An unauthorized person can masquerade as a system administrator without the proper controls, or rogue devices can connect to the network and mirror a valid device [34].

3) Data theft

Databases are an attractive target for cybercriminals, mainly if they contain personally identifiable data that can be sold or passwords that allow them to access the physical or intellectual property [34].

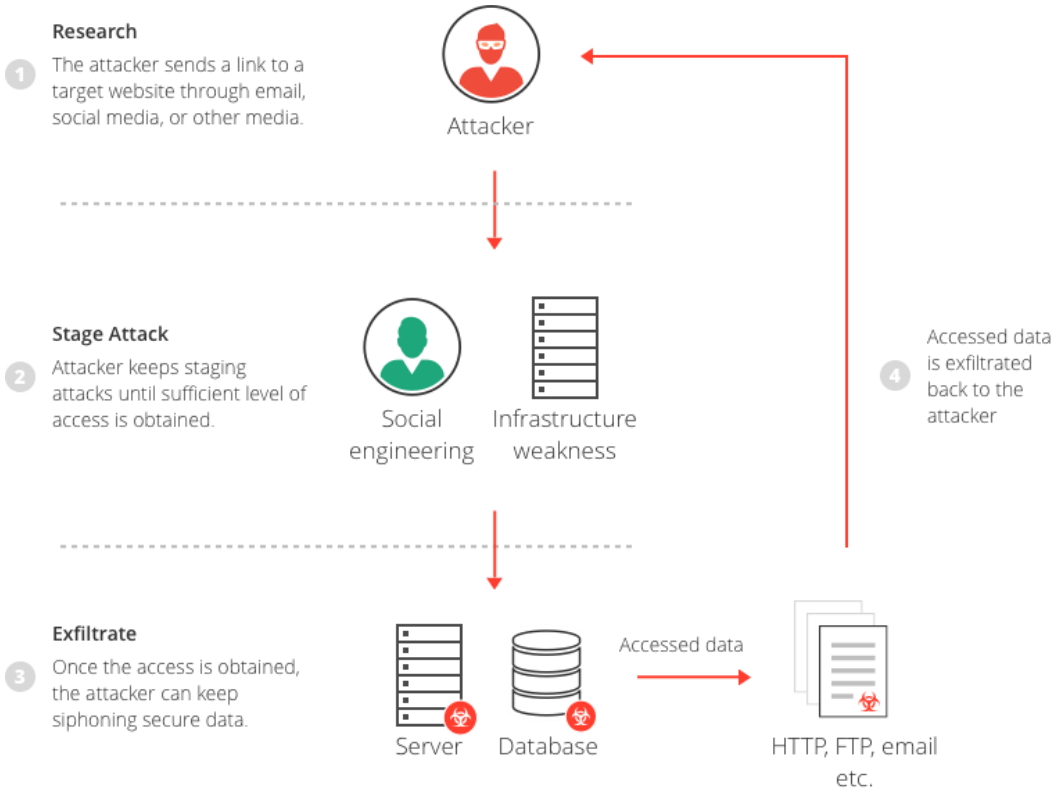


Figure 69. Data theft

Source: https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/04/what-is-data-breach.png

Data Theft may involve leakage of data, often known as exfiltration, illegal data copying, or sharing, without affecting the source data. In other situations, data theft can lead to complete data loss like ransomware attacks that involve hackers encrypting data to block access by the owner [34].

b) Security threat in the area of the "Network"

Smart networks can face advanced, stealthy attacks that can avoid traditional methods of detection such as:

4) Botnets

Robot networks, recognized as botnets, have a diverse past. In fact, a bot is simply a series of scripts, commands, or software designed to connect to something, usually a server, and perform different functions. While bots do not need to be harmful, some malicious programs set up a botnet system once a network has been breached. The result is a command-and-control architecture that can spread infection throughout the network, making cleanup considerably more challenging and potentially much more significant damage [34].

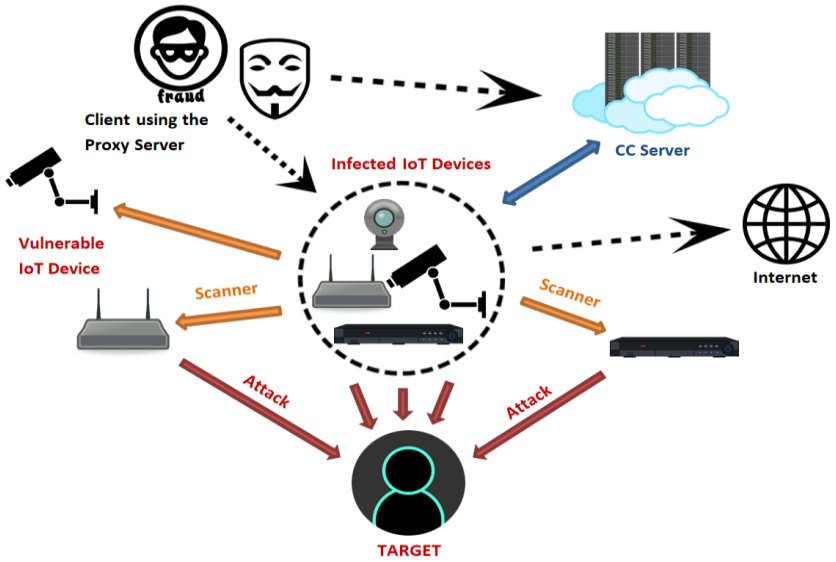


Figure 70. Botnet spreading the infection

Source: https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers/_jcr_content/root/responsivegrid/image.img.png/1519435991468/mirai-bot-0.png

5) Denial of Service Attack (DoS)

In which, for a certain period, an attacker can make a network fail by sending out an abundance of requests and unnecessary data that slows it down to the point of being useless. Many cybercriminals or machines typically involve making a distributed denial-of-service (DDoS) attack on a network. Usually, these attacks are made using botnets (remote computers under their control) to attack the site with multiple requests. Cybercriminals create botnets by sometimes infecting hundreds or thousands of computers with malware, which allows them to control the machines, enabling them to stage their attack [34].

6) Hackers

Several criminals attempt to access networks by using "brute force." It is basically the high-tech version of attempting every combination of passwords within the organization's parameters to prevent the verification of login credentials [34].

c) Security threat in the area of data centers and the cloud

Like the previous potential threats discussed, the data centers and cloud also face the same. Furthermore, data center and cloud infrastructure with a large footprint of attacks, such as servers and storage, may be susceptible to more attacks includes [34]:

7) Web attack

Web pages utilized by stakeholders to interface to smart buildings should be protected, in addition to malware and data theft. With the growth and evolution of the web, web-borne malware attacks keep pace, threatening networks, and crucial information. In contrast, McAfee Labs recognizes hundreds of thousands of new malwares every day, and the majority are transmitted through the web [34].

3.2 Challenges for smart buildings

1) Scalability

The smart buildings may span large areas and involve a significant number of smart devices and objects. It will make it hard to achieve possible security solutions, such as key management and authentication [35].

2) Mobility

With mobile devices like electronics cars and on the field technical agents, there will be a continuous requirement for authentication and secure communication with a changing environment, including smart meters, electric charging stations, and many more [35].

3) Legacy systems

Systems and devices that have already deployed could have some or no protection support since they were mainly based on proprietary technologies (hardware and software), implemented on isolated islands without communication or via private communication networks. Integrating these legacy systems into the IoT based Smart buildings is a real challenge, as, in most instances, there is no way to replace or upgrade them with modern methods to support the required security solutions [35].

4) Constrained resources

Many smart buildings, the massively deployed ones, are resource constrained. When developing security solutions, specific care must be taken to ensure that their limited resources can accommodate the solutions. It makes applying traditional security solutions a challenge, particularly those based on public-key cryptography or PKI [35].

5) Heterogeneity

Due to the difference in the resources of the objects on the smart buildings (memory, computation, bandwidth, energy autonomy, and time-sensitivity [35].

Also, their implemented protocols and communication stacks (for non-IP devices), achieving secure end-to-end communication, is a challenging task, requiring the most frequent adaptation of existing solutions or even the use of gateways [35].

6) Interoperability

It may be considered as one of the consequences of heterogeneity of protocols and communication stacks, between a device in the smart buildings. Legacy systems and devices not capable of supporting TCP / IP stack (e.g., Zigbee v1, HART) could not communicate with IP-based systems and devices except through gateways, making secure communication from end to end impossible. It was also possible to see interoperability between two devices implementing the same protocols and communication stacks, but different features: one with full support, the other with partial support (ex, DTLS with/without certificate support) [35].

3.3 Security solutions for smart buildings

There is a need for some security implementation to resolve these security issues in various areas of a smart building. Property owners and managers will quickly get overwhelmed by the scope and difficulty of securing an intelligent building. Therefore, to help bring the context to cybersecurity, the relevant security product types are divided into three categories as Good, Better, and Best [34].

In the following section, there is a brief description of these types of products and the risks they can mitigate.

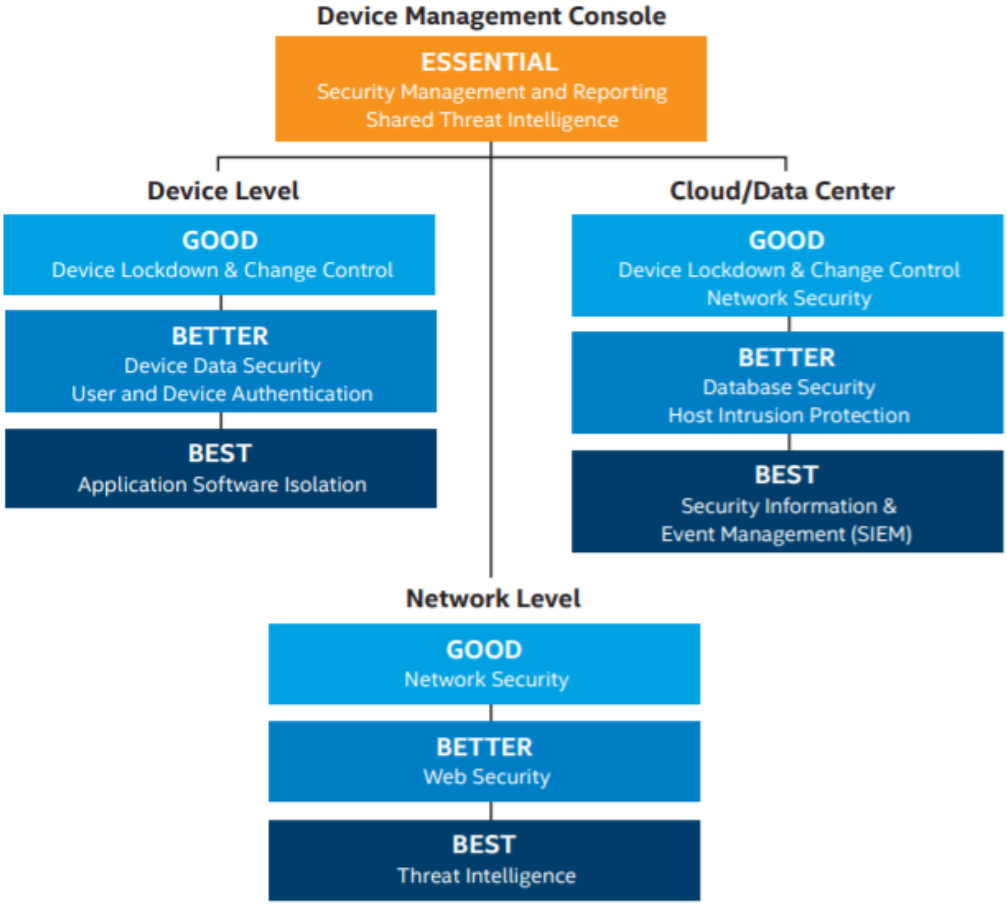


Figure 71. Types of security product are that available in the market and categorized by Good, Better and Best

Source: https://cdrdv2.intel.com/v1/dl/getcontent/334327

I. Device Management Console

Building management systems should have a central console that offers a centralized view of the security posture across the company's assets, including system, data, customer, network, and data center visibility generated by the BMS solution vendor [34].

- Security management and reporting (Good)

Simplify security operations, identify vulnerabilities, and use device management software with automatic management capabilities to take immediate action when required. Configure warnings and protection responses based on the type and criticality of smart building security incidents and establish automated workflows between security and IT operations systems to fix outstanding problems quickly [34].

For instance, Wind River Helix is a ready-made Cloud Device, cloud-based Internet of Things (IoT) framework that drastically reduces the building complexity and carrying out embedded device networks on a large scale [34].

- Shared risk intelligence (Best)

Integrate multi-source security information such as firewalls, gateways, networks, servers, and building systems and have them function like one. Automatically generate self-learning, contextual information that identifies threats, and adapts quickly. Also, optimize security when the devices can collectively learn about risks [34].

For example, McAfee Threat Intelligence Exchange maximizes the detection and reaction to threats by blocking the gap from malware exposure to containment from days, weeks, and months to milliseconds. Additionally, McAfee Data Exchange Layer (DXL) integrates multiple sources of vulnerability information and exchanges this data immediately with other interconnected security solutions, including third-party solutions [34].

a) Device Level or Stakeholder Devices

Security devices that are installed onto building systems and stakeholder devices.

- Device shutdown and change control (Good)

Disable malware as well as unauthorized programs and alterations to building systems. Minimize security threats by monitoring what's going on and securing the memory on building systems [34].

For example, to defend against malware attacks, McAfee Embedded Control employs a simple, lightweight, and highly effective whitelisting technology [34].

- Secure information system (Better)

Safe from the exploitation of mission-critical and user data and intellectual property retained by the network, storage, or building systems. Also, gain insight into how smart building information utilizes and how it can leak out. Encrypt data created to make it unreadable and unusable if malware or a hacker gains access. Prevent the illegal use of portable storage devices for safety. Ensure that the software running on the IoT gateways or IP-connected edge devices transfers data digitally signed or encrypted tunnels such as SSL / HTTPS to the data center or cloud [34].

- Client and system authentication (Better)

Enable safe and user-friendly access to information essential to business. Give users some attempts to enter their password and lock the device if it fails to stop hackers using brute-force login attacks. Authenticate devices that can connect to the network only for those who are authorized [34].

For example, McAfee Enhanced Infrastructure Protection for Intel® IoT Gateway verifies user identities, secures the network with a stateful firewall, and enables SSL / TLS tunnel management to allow safe device-to-device and device-to-cloud connection [34].

- Isolation of the devices and application software (Best)

Prevent unintentional encounters between applications running on a building system, such as an application probably malware that accesses the memory space of another and corrupts or steals its data [34].

For example, Intel Security Enterprise Infrastructure Protection (Intel® Security EIP), Separates the platform's security management features from operational applications so that the operational layer can be protected, tracked, and handled. This sophisticated approach is user-friendly, cost-effective, and integrates with both new and existing infrastructures [34].

b) Network level

Network security forbids system access through the network itself. It is the method to restrict access to a private network at its points of entry. These include firewalls, antivirus applications,

frameworks for intrusion detection and prevention, and programs for security information and event management. Furthermore, this protection handles access from outside of the network [34].

- Network security (Better)

Detect and eliminate advanced risks with intrusion prevention systems (IPS). To counter botnet and DoS threats, conduct an in-depth analysis of network traffic. Identify malware with an analysis of behaviors.

For instance, McAfee Network Security Platform helps to prevent further intrusions, identify and correct breaches more quickly and improve protection and efficiency [34].

- Web security (Better)

It holds an intelligent building gateway free of viruses and malware. It Conducts a thorough review of information uploaded into the portal. Usually, web security gateways can install multilayered protection and pattern-based malware scanning. Still, some may include additional behavioral engine-based security services to identify unknown risks based on code behavior. These can also search smartphone code and identify threads embedded in scripting languages in HTML as well as in PDF, office documents, or flash. These can also contribute to secure portals by controlling access depending on the client's geo-position submitting a request and can serve as a reverse proxy to provide AAA features and SSL protection while operating as a reverse proxy [34].

For example, McAfee Web Protection, it scans the web traffic of all the devices, users, and locations for common viruses and zero-day malware [34].

- Threat intelligence (Best)

Identify when malware writers use packing to alter or hide the composition of the code to avoid detection.

For example, McAfee Advanced Threat Defense Detects targeted attacks and exchanges threat information between management, networks, and endpoint devices [34].

c) Data center and the cloud

Data Center and cloud are increasingly targeting attacks as they house large amounts of corporate data and are also critical to perform daily activities. Device Lockdown, Change Control and Network Security are good solutions for this area which has been explained in Device Level and Network Level [34].

- Data security (Better)

Keep databases secure and accessible. Improve visibility of all database activity, including local user privileged access and advanced database attacks. Terminate sessions that violate security policy, thus providing a clear audit trail of all user activity in the database [34].

For example, McAfee Database Security gives real-time security and enforcement with business-critical databases without downtime [34].

- Host intrusion protection (Better)

Defend against existing and new zero-day threats from the data center and cloud servers. Examine queries from the database to avoid attacks, such as SQL injection. Ensure regular behavior and prevent data tampering by using shielding policies and rules [34].

For example, McAfee Host Intrusion Prevention for Server increases server security and reduces costs by reducing patching frequencies and urgency [34].

- Security Information and Event Management (SIEM) (Best)

Gain real-time insight on all devices, networks, databases, and applications in all activities. Identification of stealthy threats by real-time situational awareness. Also, use data analytics to transform data analysis and network traffic into protection intelligence [34].

For example, McAfee Enterprise Security Manager provides a real-time understanding of the outside world like threat info, reputation feed, and vulnerability level [34].

Furthermore, Cloud-based data centers, such as Microsoft Azure or Amazon AWS, may need a targeted security solution for a lifetime to guard the associated assets [34].

Eventually, the smart building industry is at that point where cybersecurity is not an option. It is a requirement. Cyber-criminals are already targeting buildings, and this is expected to increase with time. Cybersecurity, in general, can be complicated; building managers are not IT professionals, so training may be required to consider cybersecurity in the solutions. Building managers must work with their IT teams to ensure that their strategies provide safety. Also, Companies that have no IT departments should ensure that their cloud service providers comprehend cybersecurity in their solutions [34].

3.4 Pros and Cons of IoT based smart buildings

IoT based Smart Buildings give many advantages which have made life more desirable and easier. However, there are some shortcomings as well which is making the building automation hard to achieve. Some explain briefly following:

3.4.1 Advantages

1 Real-time maintenance and Problem solving

Mechanical and electrical machinery fails and may remain broken for extended periods; sometimes, even the facility staff do not know that it is broken. However, with a loT, building managers no longer need to move around manually and search for issues or react responsively to occupant's complaints. Ultrasonic or vibration sensors in HVAC systems may store data, which can detect performance differences and then warn facility managers that the issue is emerging, all in real-time. The ductwork of the HVAC system is essential for overall performance [36].

It can be tracked effectively, accurately, and in real-time using sensors installed. Within duct systems, IoT solutions provide continuous data on airflow, temperature, and pressure. The gathered data can be used to plan maintenance renovation or redesign, while at the same time adding value to the investment and increasing the HVAC system's useful life [36].

2 Devices connectivity

Most of today's buildings have powerful internal networks or automation systems that connect to devices executing useful functions. By connecting these networks and devices, the purpose of IoT is to monitor and gain new information to solve problems and automate functionalities [36].

Moreover, smart Hive and Nest thermostats are just the start. By linking various components of the HVAC systems and installing communicating sensors, air, and temperature quality control could be limitless. For example, a smart system will minimize airflow when no one is inside the building, saving energy and money. Sensors installed into air purifiers will detect pollution levels in the building environment, reacting by cleaning the air as efficiently as possible, saving on hours of daily usage. Energy companies are continually tailoring the power costs throughout the day, so it costs most when it is in the highest demand. A connected thermostat will change the temperature to those rates automatically, while at the same time providing maximum comfort and cost savings for the consumer [36].

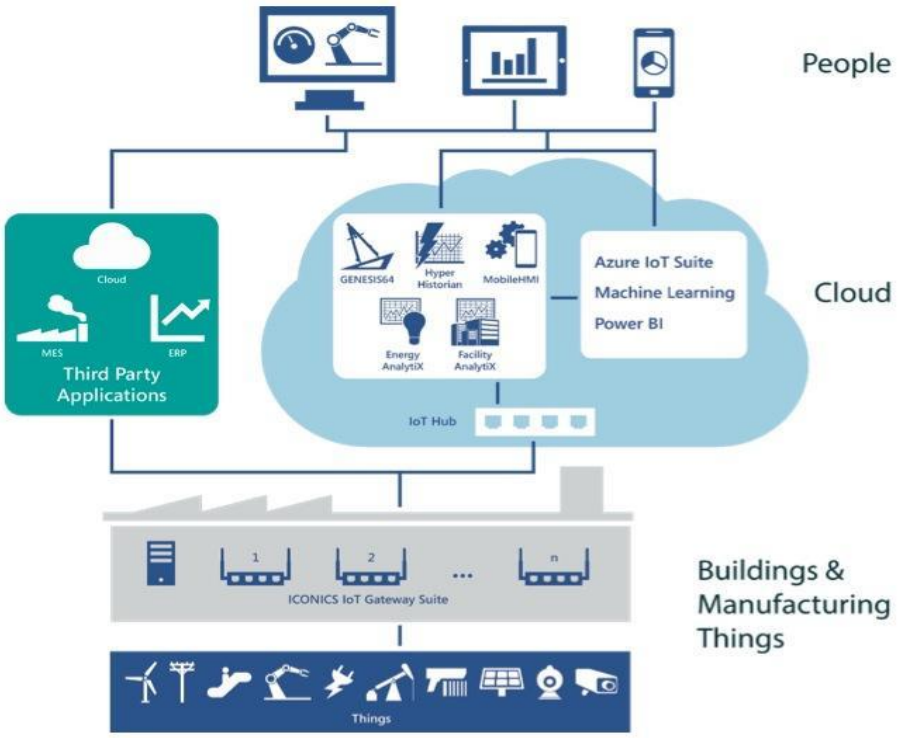


Figure 72. Devices connectivity

Source: https://iebmedia.com/images/art_images/IEB95_p16_2.jpg

3 Efficiency and Comfort

Commercial buildings must adhere to the industry standard for thermal comfort for tenants, and (according to surveys) often fall short on this goal. Factors affecting the temperature and air quality of a building include occupancy variations coming in and out seasonal air quality and temperature

of the building, the presence of chemical and biological hazards in the fresh air entering the building, and fluctuations in "hot spots" named functional spaces, conference rooms, and auditoriums [36].

Although with fully automated thermostats and building systems, under many complicated circumstances, a building engineer has no way to make real-time changes. Also, commercial buildings are responsible for 40 percent of global greenhouse gas emissions. Some technological innovations (including modern HVAC systems) have made progress towards greater efficiency. Nevertheless, using data analytics from building automation systems to enable facilities managers to make real-time changes will significantly reduce energy consumption, increase occupant satisfaction, and save on operating costs [36].

4 Moving Maintenance to a different level (from proactive to predictive maintenance)

In which, sensing inputs help capture real-time diagnostics that can be aggregated and mined for advanced study and error detection. Besides, Users can then modify their processes, gather performance data, and arrange the data into different reports. With this additional insight into the network, users will be able to see improvements and issues that may be used for predictive maintenance within systems or individual devices [38].

As buildings have multiple systems in use each day, maintaining a proper maintenance plan and maximizing the performance of each device can be challenging. It is because so many factors affect its efficiencies, such as temperature, the quantity of use, and climate. Earlier, maintenance workers have implemented either a calendar-based maintenance schedule or a reactive maintenance schedule, where devices are repaired or replaced only after a system failure [38].

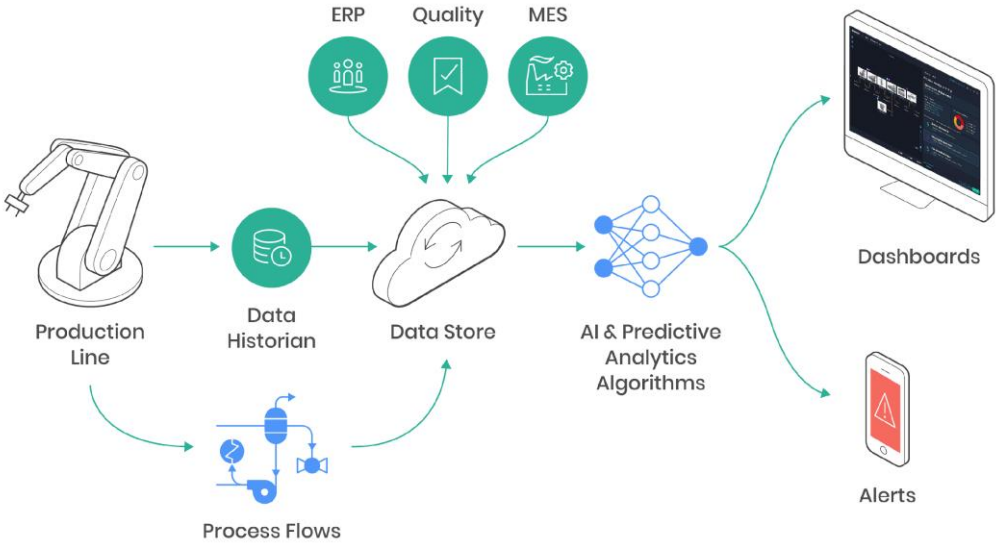


Figure 73. Predictive maintenance in smart buildings

Source: https://xhtnh2f75kp4la0u3slg1e1d-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/Predictive-Maintenance-1.png

3.4.2 Disadvantages

1 Cybersecurity and User data theft

Despite 200 billion connected devices by 2020, and by 2021 overall IoT technology business investment is approaching $6 trillion, IoT is increasing at an unprecedented rate. It results in significant privacy and safety threats for the customer: mobile devices, complicated connected system networks, amount of data collection, and user encryption. It needs an appropriate and comprehensive operating backup plan for smart building systems in case of either a cybersecurity attack, a natural disaster, or other temporary service interruption [36].

A business may need to hire a consultant who can determine the threat hierarchy through building systems, stakeholder device (user access), and interlinked data centers, and then create a comprehensive risk management strategy for protection. This strategy would need to consider the physical protection of IoT systems and a complex cybersecurity model for integrating remote cloud infrastructure, firmware, and authentication security [36].

Furthermore, the threat of cyber-attacks is an unquestionable and prominent limitation on the adoption of IoT. According to a Gemalto survey released in October 2017, an overwhelming 90 percent of consumers lack confidence in IoT device security. In contrast, the 2017 IoT research report by Aruba Network showed that 52 percent of respondents thought that external intrusion is the greatest threat to their IoT devices, and surprisingly, 84 percent had already encountered an IoT-related breach [37].

According to this report, IoT continues to grow, and tighter security standards have to be adhered to by all stakeholders, this will require increased funding, as well as more emphasis on device visibility and security compliance at all levels of the technology stack. To improve customer trust in this area, IoT device manufacturers and service providers must need to raise spending on-device protection [37].

2 Privacy

There are significant privacy issues concerning the collection storage and use of personal data. Whenever the collection and use of IoT data involve personal information, and when the collected information can be used to forecast an individual's actions, companies can face a potential privacy issue. It is particularly problematic for buildings that use IoT devices, because of their purpose to sense occupants ' activity and monitor behavior to help facility managers make better use of their space [37].

Users need reassurance that their data is used safely and kept secure, and the ability to opt-out of surveillance must always be easily accessible. Also, organizations need to decide how to protect data privileges and control data access. A company may own the device that collects data, but the data belongs to the user, so companies need to be more cautious and careful about how data is handled [37].

3 Device compatibility

As more devices and HVAC components from different manufacturers are integrated, the issue of compatibility occurs when tagging and monitoring. While this drawback may not be as big a problem if manufacturers adhere to a common standard, still technical problems will persist afterward [36].

To order to be effective, IoT needs an advanced and wide variety of technology collaborators to work together. It can prove challenging to link to smart thermostats, data centers, and other mobile networks for improved efficiency and return on investment for buildings with traditional HVAC equipment that still has a useful life. Any device or equipment malfunction or bugs could have severe consequences and liabilities for building operation and health for the residents [36].

4 Cost and Training

Cost is one of the barriers to implementing IoT technology, especially for large, square footage or portfolio investments. Usually, this can range from the hundreds of thousands for simple light and cool sensors to the millions for robust protection and operating equipment [36].

Many office leases are designed to pass on all utility-related expenses to tenants who are unwilling to spend extra on upgrades, especially if initial expenditures will take years to recover. Many times, allocations for upgrades and apartment enhancements are capped, so tenants may choose to invest in more traditional features [36].

The tremendous real-time data collection capacities and opportunities for energy consumption for energy automation also come to user adoption and training. After all, if data are not used to optimize HVAC and thermostat capacity for convenience, indoor air quality, and energy efficiency, then the initial installation costs are not worth it. Before these functions are entirely fully automated, facilities managers must need to be a link among interpreting data and managing building settings and critical repairs. It can contribute to high learning curves and the need to train staff or hire additional support staff, and contribute to the deployment costs [36].

3.5 The future scope of IoT based smart building

Trends in the Smart Buildings Market with the costs of connected sensors and continuously decreasing cloud computing, IoT devices are becoming increasingly common that intelligently monitor and control building operations [40].

It is anticipated that approximately 10 billion devices will be installed in buildings by 2020, making it one of the world's fastest-growing sectors. Consequently, the smart building market is likely to rise from an $8.5 billion size in 2016 to around $58 billion worldwide by 2022 [40].

However, there are some actual implications for the real estate market when it comes to the smart building revolution. Which will change the way buildings are managed in the coming years, helping businesses save energy and expenses, offer improved tenant experiences, and achieve higher property values. These are explained briefly in the following sections [40]:

i. Air quality monitoring

Since most of us spend more than 90 percent of our time indoors, good quality indoor air is essential to resident safety and productivity. A study by Harvard discovered that "people who work in well-ventilated facilities with indoor pollutant and CO2 levels below average have significantly higher cognitive function scores." Therefore, buildings will gradually be designed with wireless sensors monitoring CO2 levels and dangerous small particles, issuing alerts, and adjusting ventilation if required. And they're not just going to monitor the inside. In countries with intense pollution, monitoring the quality of the outside air that comes in through ventilation is equally important. Intelligent systems can suggest which filtres to replace and decide to switch off the system if the external air quality is critically dangerous [40].

ii. Smart lights

One of the greatest revolutions along the way we light our buildings has been the discovery of LED lighting for about thirty years. The LED light uses less than 80 percent of traditional bulb electricity and has a lifespan of 10 times more. Also, today's LEDs make up just 10 percent of all lighting systems, so many buildings have an easy opportunity to save energy and expense only by switching bulbs. Smart lighting that adjusts according to occupant preferences (also called human-centric lighting) will be one of the most significant lighting trends for buildings moving forward. These intelligent lighting systems can imitate the natural light progression of daylight in order to follow our circadian rhythm or change its intensity according to distinct tenant requirements. In an office, brighter lighting can be used after-lunch to help motivate staff in the office area, whereas gentle light in hospitals can help patients to relax [40].

iii. Security in smart building

Connected IoT systems deployed throughout the building help facility managers to maintain their building secure. The most crucial of these devices are cameras and access control systems such as

badge readers, enabling unwanted visitors to be spotted and granting permission to employees to visit workers. IoT devices also have additional security advantages inside buildings. We will, for example, it can help building managers figure out if any doors are being kept open regularly or if an alarm has gone off falsely. A brilliant security system could even communicate to other devices that some workers left the building, causing the lights to be shut down [40].

iv. Cybersecurity importance

The smarter a building gets, the more vulnerable it becomes to cyber-attacks. The growing presence of internet-connected devices within a structure makes it easier for outsiders to place viruses, theft data, or hack into networks. Indeed, the Gartner Institute estimates that approximately 20 percent of all smart buildings will have suffered from some form of digital attack by the end of 2018. Cybersecurity will be a crucial issue for the development of the real estate sector. Building operators need to stay ahead of potential threats and take action to improve their cybersecurity, such as enhancing authorization controls and implement data encryption and working closely with their IT department [40].

v. Resident control

Smart buildings allow their inhabitants more control of the building. Users can now communicate directly with a building by adjusting the temperatures, reserving meeting rooms, or adjusting the lighting, all from one central location and according to their needs. It provides a much more private and enjoyable atmosphere (like in a hotel) but can also offer energy-saving advantages, for example when meeting rooms switch off lighting automatically when nothing is booked. At the same time, a smart building will give occupants convenient ways to send reviews to facility management, for instance, when something is damaged or needs to be reordered [40].

vi. Smart parking

Smart systems are not only installed where individuals live and work but also the structures around them. Parking spaces inside and near the building where there are lots of potentials to make things intelligent is one example of this. Cameras and sensors will identify free parking spaces and transmit this information to commuters, eliminating extra laps and unnecessary use of gasoline. Ideally, this information is shared across multiple systems so that staff also get details from public

streets on parking spots. Other options include allowing visitors to reserve parking spaces for frequent users in advance, or by automatic online payment systems [40].

vii. Focus on wellbeing

Most enterprises understand that their employee's health and comfort is a crucial differentiator that influences productivity and workplace satisfaction. Therefore, considering how a building promotes its occupants ' wellbeing will be a significant trend for the future [40].

Another indication of this is the growing significance of WELL Building Certification (launched in 2014), the world's first building standard focused entirely on human health and wellness. This score building along with specific categories such as air water, health or mind, requiring for example, that workplaces are not too busy, that childcare is on-site, and there are natural elements such as trees. WELL is in close partnership with the LEED Sustainable Building Certification, so that buildings can be accredited as healthy and green at the same time [40].

viii. Evolution of Building Management Systems (BMS)

In "Building Management Systems" (BMS), computer-based systems for monitoring and controlling services such as lighting, heating, and ventilation, everything that goes on inside a building can come together. These systems are not new and have existed for decades. But while they were previously highly fragmented and operated independently, a modern BMS makes all operations of the building visible in one place [40].

This type of system gathers all available building data continuously, filters it through an analytics layer, and helps facility managers decide. Such systems are becoming truly smart, like everything else inside the company, by making recommendations and encouraging administrators to respond much more proactively to potential problems [40].

In the planning and construction phase too, technology is disrupting the real estate industry. One of the most prominent developments here was the rise of Building Information Modelling (BIM), a new method of planning and working where a project's digital 3D model is created before actual construction. Architects, planners, and subcontractors all collaborate in the BIM process to build

a complete virtual building layout, which allows planning more effectively and transparent and saves time and mistakes afterward [40].

ix. Bundling

Today investors, tenants, and operators face an almost overwhelming number of options for making their building smarter. Some may choose to update just some systems at first and upgrade the others slowly to reduce costs. However, as with other sectors, another purchasing approach is becoming more common in the industry, namely bundling [4o].

Organizations achieve cost and time savings by bundling various smart technologies and purchasing them at once, as well as profits from products operating in synergy. Bundling can also be used to redesign old buildings and has shown those cost savings of up to 15 percent can be accomplished. Now, there are specialized consultancy companies who make recommendations about which devices to purchase together and provide as-a-service pricing models for intelligent systems to save upfront costs [40].

4 Case Study: Design and Technologies for implementing a smart educational building

I. Introduction

This case study explains the design of a smart education building and the innovative technologies that have been executed. In which, the building was designed as both a model of how new technologies can significantly minimize the energy requirements of large-scale university buildings and provide a "living laboratory for students and faculty to see how these systems work and interrelate. It was a LEED Platinum-Certified "Engineering East" Building. Engineering faculty have been involved in the creation of state-of-the-art engineering laboratories by providing feedback to the builder [41].

According to this case study outlines different approaches and related technologies in designing smart buildings. In designing the smart educational building and delivering research ability, this building is designed with hundreds of different sensors that monitor everything from the temperature of the cold water entering and exiting the building, the amount of electricity generated by the solar panels and CO2 level in a lab. The study gives an overview of the numerous advanced systems introduced in this new "Smart Green Building." It illustrates the different sensors and data available for monitoring these devices, both in real-time and by storing and processing such data by data mining routines. It includes many sections that were used for designing as well as implementing the smart educational building, which is as follows [41]:

1) This building was LEED or Leadership in Energy and Environmental Design green building certified for improving environmental and human health performance. Where LEED addresses all forms of building and highlights state-of-the-art approaches in five areas [41]:
   i. Sustainable and Development
   ii. Saving water
   iii. Energy efficiency
   iv. Selecting materials and resources
   v. Indoor air quality

Also, points are given in each area as silver, gold, or platinum level of certification based on the type of project [41].

2) Main building design and Subsystems: In the main building, during implementation, some advanced technologies were utilized in the subsystems, such as [41]:
    2.1. Heating, Ventilation, and Air Conditioning (HVAC).
    2.2. Cloud computing and network control system.
    2.3. Power production system and its control.

In the Building, on the first floor, mechanical equipment and sensors were installed. The building is fitted with hundreds of sensors that monitor and capture different parameters and display them on the dashboard in real-time, which can be accessed via a web-based application called DeviceWise developed by ILS Technology. Where the DeviceWise system regularly collects sensor data from the electrical, computing, and air conditioning systems of the building and stores the data in a database. Then, the system offers a web-based app that shows the summarized details accessible from any internet browser in an energy dashboard. DeviceWise also gives an API that enables other applications to access data stored in the database outside the energy dashboard for extraction and reporting [41].

2.1. Heating, Ventilation, and Air conditioning system (HVAC)

Unlike conventional cooling systems that use air conditioning or heat pumps to eliminate hot air from a building and replace it with cooler air, here the system in this building does the opposite. Because this building was built in Florida where most of the days the buildings need to be cooled rather than heated, a campus-wide chilled water system provides cold water through the campus. It uses an advanced method to temper the chilled water to lower humidity, and other heating systems if necessary. The building contains three chilled water tertiary pumps to circulate the chilled water. Two pumps run continuously at a capacity of 50 percent in parallel. Usually, the third pump is turned off and serves as a backup to the first two pumps. The active pumps are cycled periodically [41].

As the chilled water reaches the building, some of it is first passed through a heat exchanger, which raises the water temperature by approximately 10 degrees Fahrenheit. Then, the remaining water

is pumped into the chiller frames in the building and sent to the roof to flow through the air handler units' coil [41].

Several sensors are installed all over the system to ensure that components work correctly. Such sensors include the supply and return temperatures at various locations in the building, pumps output flow and condition, the differential, and the Chilled Water Control Valve status. The hot water heating system used to heat in winter and dehumidify the building in summer comprises three different water systems: a well water system, a source water system and a hot water system. Well Water System draws water from a well that maintains a constant water temperature of about 78 degrees F. Then, the water is pumped between the New Water System and the Source Water System through a heat exchanger. The heat exchange passes heat from the Source System to the Well System or from the Well System to the Source System, depending on the temperature of the source water [41].

The Source Water System runs the water into pipes connecting into the computer server room cooling system, which consumes the heat energy from the IT device. Then, on the other side, the water heated by the servers is transferred to the Hot Water Network through another Heat Exchange Unit. After this, heat energy is absorbed by the hot water system from the source water system. Besides, when hot water is needed for dehumidification or heating above the computer room servers, the Source Water can also operate via one to three heat pumps extracting additional heat from the Source Water and transmitting the heat energy to the Hot Water System. There is one additional heat pump that is used as a back-up and the sequence of which heat pump is rotated weekly as first, second, and third [41].

Sensors monitor the temperature of the well water, the temperature before and after the first heat exchanger, the energy absorbed by the servers, and at other locations throughout the building. In addition, sensors monitor the status and operational statistics for the different pumps and heat pumps used in the process. The critical sensors used by the High-Temperature Chilled Water system include the status and performance of the two pumps, the temperature of the water entering, after the first exchange of heat, and before the final exchange of heat [41].

2.2. Cloud computing and network control system

As per this case study, the server room designs applying a "room within a room" (or hot aisle) configuration. The room is an open space of 600 square feet, cooled by fans who blow over the tempered chilled water system. The inner room consists of 14 server racks, four computer room cooling units, and an uninterruptible power system for air conditioning. The four-computer room cooling systems offered extra cooling and used the gas to liquid refrigerant configuration [41].

Moreover, the server room contains various types of sensors. Each group of sensors gathers power data from the four-computer room cooling units, including the Supply Fans and Compressor's overall Amperage. It also provides real-time information via LAN connected temperature and humidity sensors. Also, other sensors monitor the LAN traffic flow to and from the server and power used by the servers. It uses a private cloud computing system where computer laboratories and all devices in the building utilize cloud computing technologies to execute software applications and access data stored in the cloud [41].

2.3. Power production system and its control

The building produces around 4 percent of its electricity from three solar photovoltaic cell arrays. And the power generated by the solar arrays is transferred via a central power conversion device situated in the server room where the direct current from the arrays is transformed into alternating current and applied to the power grid of the buildings. Besides, the converter records the watts transmitted to the network in real-time [41].

Furthermore, sensors monitor the utilization of electricity inside the building, which is divided into various categories to analyze changes into the system, such as: Mechanical equipment (power for air handler units, pumps and air conditioning of the building), Lights (power for light the building), Receptacle(energy used by the devices plugged into the wall), Kitchen, and solar power generated by photovoltaic panels [41].

The light inside the building is controlled by a system of connected sensors and switches provided by Encelium Technologies. It contains occupied as well as unoccupied modes for lighting the main corridor, along with overrides based on the occupation of the building. It depends on sensors

and switches deployed through the building that evaluate the rule of the room using motion detection and required lighting based on ambient light [41].

Moreover, Throughout the building, the device collects feedback from the various sensors and switches, integrating that information with configurable lighting parameters then decides the best lighting for each space and region. For further analysis and research, it also records the illumination and occupancy data [41].

3) Alert and Monitor system

According to this case study, it is a part of the NSF Center project, and the university members worked with Aware Technologies and its Process Data Monitor system. It is an alert system utilizing data mining techniques to categorize sensors data into similar knowledge clusters. After defining such clusters, users can decide whether the clusters reflect normal or abnormal running conditions for the sensor data used to create the cluster. The system will then maintain track of how many times each cluster is computed, and an analytical method is used to assist with optimization [41].

It has also built data warehouses that store information from various sensor systems, like Device Wise, standalone wireless and wired sensors, PDM-calculated clusters, and weather stations [41].

Moreover, for the security of building and access control, it has facial recognition and fingerprint scanner for authorized access only [41].

Additionally, in this case study, it also analyzes the performance of various building systems to examine solar panels by tracking the power generated for one year [41].

4) Data center power utilization

As per this case study, the data center contains two racks situated in a hot aisle structure, with separate uninterruptible power supply systems used by computing blades, discrete computers, attached network storage, and networking devices. The total power the data center utilizes includes, is used by four CRACs (air conditioning units) that cool the air inside the hot aisle. The hot water chain, which utilizes heat pumps to extract heat from the hot aisle, reaches a high

temperature of 50 ° C and an average differential of 20 ° C, being fruitful in reusing waste heat for other building devices [41].

In the end, reliable instrumentation in the new LEED Platinum engineering building provides a multidimensional view of the internal workings of its HVAC and power systems. Several sensors allow a detailed analysis of the efficiency of the building system and the power usage of the data center. Furthermore, to get a more accurate picture, it is as important to consider outside factors such as weather building occupancy and school schedule. Also, this case study can be valuable to build a smart building [41].

5 Conclusion

To sum it up, it would be imperative to say that these IoT based smart buildings are very crucial for energy efficiency, flexibility, and comfort. Also, it had never been a good idea to waste energy. But there was a time when nobody realized how to minimize such waste, nor the cost of it. It covers not only the direct cost of excessive expenditure on fuel and power plants, but also affects such as pollution-related health prices, the cost to treasuries subsidizing fossil fuels, or rising global warming.[39].

Many have considered buildings to be an excellent place to start reducing these expenses. Building stock is the most voracious customer in the world as most energy-consuming countries are more significant than industrial processes or transport. And the potential for better and leaner energy use is vast. While there is no such thing as a commercial airliner with zero energy or a cement plant with zero energy, not even experimentally, zero-energy buildings are already outdated. The energy efficiency industry is well on its path from being a niche market to a well-established market with enormous potential [39].

The global market for energy efficiency is worth at least USD 310 billion per year and is proliferating, according to the International Energy Agency (IEA). It provides significant economic opportunities. Companies and governments all over the world have started to act on this. Most countries have adopted minimum energy-efficiency standards; not only member states like the US and the EU, but also many developing economies, including China. And the businesses responded by innovating and competing in order to give more efficient solutions. It has produced spectacular results in many areas, higher productivity earlier, and at a smaller upfront price than it had expected [39].

Intelligent buildings can do more than just cut the cost of energy. While their users love some buildings, others are hated. Quite often, this is because of the design of the building. The economic implications can be immense – not only in terms of rentals or sales prices but also in terms of efficiency and absenteeism of the occupants [39].

Finally, smart buildings will improve the overall energy system's efficiency and reliability. Store energy when it is overflowing, then release it and shut down non-essential use when demand is

high. Indeed, this can reduce peak loads, the need for generation capacity, and the possibility of blackouts [39]. Which leads the automation to smart cities too.

Appendix A: List of Figures

1 Introduction 6
1.1 What is the Internet of Things? 6
1.2 History and Background 9
1.3 How does the IoT system work? 11
1.3.1 Examples of IoT 13
1.4 Evolution in various sectors 15
1.5 IoT reference architecture 23
1.5.1 IoT reference architecture requirements 24
1.5.2 The Architecture 29
1.6 IoT protocols 39
1.6.1 Network protocols 39
1.6.2 Data protocols 46
1.7 IoT conclusion 50
1.8 What is a smart building? 50
1.9 History and Evolution 61
1.10 How does a smart building system work? 63
1.11 What can a smart building do? 64
1.12 SB conclusion 65
2 Correlation between IoT and smart buildings 67
2.1 Difference between IoT Smart Buildings with and without integration 73
2.1.1 Smart Building with integration 73
2.1.2 Smart Building without integration 74
2.2 Components of smart buildings 75
2.3 What makes smart buildings "smart"? 78
2.4 Non-energy benefits of smart building 81
2.5 Existing smart building technologies 82
2.5.1 Examples of smart buildings 90
3 Security issues and challenges for the IoT based smart building 99
3.1 Security issues in smart building 99
3.2 Challenges for smart buildings 104

3.3 Security solutions for smart buildings 105
3.4 Pros and Cons of IoT based smart buildings 111
3.4.1 Advantages 111
3.4.2 Disadvantages 114
3.5 The future scope of IoT based smart building 116
4 Case Study: Design and Technologies for implementing a smart educational building 121
5 Conclusion 127
Appendix A: List of Figures 129
Appendix B: Reference 131

Appendix B: Reference

[1] “Internet of Things (IoT): A Literature Review”, “Somayya Madakam, R. Ramaswamy, Siddharth Tripathi”, Journal of Computer and Communications, 3, 164-173., 2015. (online source)

https://file.scirp.org/pdf/JCC_2015052516013923.pdf

[2] “5 Intelligent Building Examples We Can’t Stop Talking About”, Elizabeth Dukes, 2018.

https://www.iofficecorp.com/blog/intelligent-building-examples

[3] “The Definitive Guide the Internet of Things for Business 3rd Edition”, “Syed Zaeem Hosain, Chief Technology Officer”, Aeris Communications Inc., 2018., (Book).

[4] “IoT Explained – How Does an IoT System Actually Work?”, “Calum McClelland”, Leverege., 2016.
https://www.leverege.com/blogpost/iot-explained-how-does-an-iot-system-actually-work

[5] “A Brief History of the Internet of Things”, “Keith D. Foote”, DATAVERSITY., 2016. https://www.dataversity.net/brief-history-internet-things/#

[6] “The Internet of Things: Evolution or Resolution?”, American International Group, Inc.

https://www.aig.com/content/dam/aig/america-canada/us/documents/insights/aig-white-paper-iot-english-digital-brochure.pdf

[7] “Flight Control and Fly-By-Wire”, “Ahmedavionics”, 2013.

https://fcs4987.wordpress.com/2013/12/08/flight-controls-and-fly-by-wire/

[8] “How IoT is Transforming The Future of Healthcare”, Keysight Technology.

https://www.keysight.com/ca/en/assets/7018-06186/white-papers/5992-3024.pdf

[9] “A Reference Architecture for the Internet of Things”, “Paul Fremantle”, WSO2, 2015.

https://wso2.com/whitepapers/a-reference-architecture-for-the-internet-of-things/

[10] “The Internet of Things Reference Model”, CISCO, 2014. (online source)

http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

[11] “IoT Management”, EDUCBA, 2019. (online source)

https://www.educba.com/iot-management/

[12] “Untangling the Potentials of IoT Protocols and Standards”, Kellton Tech, 2020. (online source)

https://www.kelltontech.com/kellton-tech-blog/internet-of-things-protocols-standards

[13] “IoT Technology and Protocols – 7 Important IoT Communication Protocols”, DataFlair, 2018.

https://data-flair.training/blogs/iot-technology/

[14] “Do you use the Z-Wave protocol for home automation? Which smart home application have you adopted?”, “Margaret Rouse”, TechTarget, 2018.

https://internetofthingsagenda.techtarget.com/definition/Z-Wave

[15] “Top 15 Standard IoT Protocols That You Must Know About”, UBUNTU PIT, 2020. (online source)

https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/

[16] “IOT drives efficiency tech development in smart buildings”, Tristan Van Iersel, 2016.

https://fintk2.com/iot-drives-efficiency-tech-development-smart-buildings/

[17] “What is Smart a Building”, Building Efficiency Initiative, 2011. (Article, online source)

https://buildingefficiencyinitiative.org/articles/what-smart-building

[18] “A Brief History of Smart Buildings”, ACS, 2019. (online source)

https://acssmartbuildings.com/a-brief-history-of-smart-buildings/

[19] “Design and Implementation of Intelligent Building / Smart Building”, Dipak Patel, 2017.

Source: https://digital.library.ryerson.ca/islandora/object/RULA%3A6887/datastream/OBJ/view

[20] “The Ultimate Guide to Building Automation”, Control Solution INC, 2015.

https://controlyourbuilding.com/blog/entry/the-ultimate-guide-to-building-automation

[21] “Connecting the Smart Building of the Future”, “Glenn Colpaert”, 2018.

https://www.codit.eu/blog/connecting-the-smart-building-of-the-future/?country_sel=be

[22] “How Smart Building and IoT Trends of 2018 is Shaping The Future of Construction”, Paul L. Smith, 2019.

https://wncgreenbuilding.com/smart-building-and-iot-trends-2018/

[23] “Making Buildings Smarter”, JEFF DORSCH, 2018.

https://semiengineering.com/buildings-get-smarter-through-tech/

[24] “Design and Implementation of Intelligent Building / Smart Building”, Dipak Patel, 2017.

https://digital.library.ryerson.ca/islandora/object/RULA%3A6887/datastream/OBJ/view

[25] “5 Features for Smart Building”, Amotus. (online source)

https://amotus-solutions.com/article/31-5-features-for-smart-buildings

[26] “Smart Building can be a leading light in the IoT”, Caroline Hayes, 2019.

https://www.electronicsweekly.com/blogs/led-luminaries/led-design/smart-buildings-can-leading-light-iot-2019-02/

[27] “Overview | Smart HVAC systems in buildings and energy savings”, Francois Duirer, 2017.

https://www.buildup.eu/en/news/overview-smart-hvac-systems-buildings-and-energy-savings-0

[28] “7 Smart Building Technologies Needed to Bring Facilities into the Future”, Hugues Meyrath, 2019.

https://servicechannel.com/blog/7-smart-building-technologies/

[29] “5 Examples of Smart Buildings”, Raphaelle Jerez-Grisel, 2018.

https://www.bimandco.com/en/blog/5-5-examples-of-smart-buildings

[30] “Bahrain World Trade Center”, Design Build Network. (Online source)

https://www.designbuild-network.com/projects/bahrain-world-trade-centre/

[31] “Smart Buildings: Using Smart Technology to Save Energy in Existing Buildings”, Jennifer King and Christopher Perry, 2017.

https://aceee.org/sites/default/files/publications/researchreports/a1701.pdf

[32] ”7 Incredible Smart Buildings”, Planet Technology USA ,2019.

https://planetechusa.com/7-incredible-examples-of-smart-buildings-and-what-makes-them-smart/

[33] “What Makes a Smart Building ‘Smart’?”, JM Electrical, 2014.

https://www.americaninno.com/boston/what-makes-a-smart-building-smart-1/

[34] “Security Practices for Smart Buildings: Good, Better, Best”, Intel, 2016. (online source)

https://cdrdv2.intel.com/v1/dl/getcontent/334327

[35] “Security Issues and Challenges for the IoT-based Smart Grid”, Chakib Bekara, 2014.

https://www.sciencedirect.com/science/article/pii/S1877050914009193

[36] “Pros Vs. Cons of implementing IoT Programs in your Facility”, Therma, 2019.

https://www.therma.com/pros-vs-cons-of-implementing-iot-programs-in-your-facility/

[37] “What the main challenges preventing the adoption of the IoT in Building”, Memoori, 2018.

https://memoori.com/main-challenges-preventing-adoption-iot-buildings/

[38] “Connected Buildings and Predictive Maintenance”, Building Logix, 2020.

https://buildinglogix.net/connected-buildings-predictive-maintenance/

[39] “Smart Buildings – Combining energy efficiency, flexibility and comfort – White paper”, ResearchGate, 2015.

https://www.researchgate.net/publication/282815708_Smart_Buildings_-_Combining_energy_efficiency_flexibility_and_comfort_-_White_paper

[40] “The Future of Smart Building – Top Industry Trends”, Blue Future Partners, 2018.

https://medium.com/blue-future-partners/the-future-of-smart-buildings-top-industry-trends-7ae1afdcce78

[41] “Design and technology for implementing a smart educational building: case study”, ResearchGate, 2016.

https://www.researchgate.net/publication/303392524_Design_and_technologies_for_implementing_a_smart_educational_building_Case_study

[42] “Smart Building Market Worth 31.74 Billion USD by 2022”, MarketsandMarkets, 2017.

https://www.prnewswire.com/news-releases/smart-building-market-worth-3174-billion-usd-by-2022-641403563.html