Review

The Future of Emerging IoT Paradigms: Architectures and Technologies

Abdul Salam 1*, Anh Duy Hoang 2, Atluri Meghna 3, Dylan R. Martin 4, Gabriel A. Guzman 5, Yung Han Yoon6, Jacob B. Carlson 7, Jordan L. Kramer 8, Keim Yansi 9, Michael G. Kelly 10, Michael J. Skvarek 11, Milos Stankovic 12, Nguyen Dang Khoa Le 13, Tyler A. Wierzbicki 14, Xiaozhe Fan 15

1 Purdue University; salama@purdue.edu
2 Purdue University; hoang15@purdue.edu
3 Purdue University; atlurim@purdue.edu
4 Purdue University; mart1243@purdue.edu
5 Purdue University; gaguzman@purdue.edu
6 Purdue University; yoon127@purdue.edu
7 Purdue University; carlso80@purdue.edu
8 Purdue University; kramer60@purdue.edu
9 Purdue University; ykeim@purdue.edu
10 Purdue University; kelly258@purdue.edu
11 Purdue University; mskvarek@purdue.edu
12 Purdue University; mstankovic@purdue.edu
13 Purdue University; le82@purdue.edu
14 Purdue University; twierzbi@purdue.edu
15 Purdue University; fan115@purdue.edu

Abstract: With Internet of Things (IoT) gaining presence throughout different industries a lot of new technologies have been introduced to support this undertaking. Implications on one such technology, wireless systems allowed for the use of different communication methods to achieve the goal of transferring data reliably, with more cost efficiency and over longer distances. Anywhere from a single house with only a few IoT devices such as a smart light bulb or a smart thermostat connected to the network, all the way to a complex system that can control power grids throughout countries, IoT has been becoming a necessity in everyday lives. This paper presents an overview of the devices, systems and wireless technologies used in different IoT architectures (Healthcare, Vehicular Networks, Mining, Learning, Energy, Smart Cities, Behaviors and Decision Making), their upbringings and challenges to this date and some foreseen in the future.

Keywords: IoT in Healthcare, IoT in Vehicular Networks, Behaviors and Decision Making, IoT in Learning Environments, IoT in Mining, Io IoT in Energy Systems, IoT in Smart Cities, Sensors, Low Power Networks

1. Introduction

Of all the emerging technologies Internet of Things (IoT) is expected to revolutionize the way the world operates in future. It is going to connect all the devices through giant networks which can interact, analysis, and take smart decisions with minimal interaction from the humans. IoT along with other Artificial Intelligence (AI) and Blockchain is going to transform the businesses, leisure, health, and society.

1.1 The Origin of the Internet of Things (IoT)

The phrase internet of things was first thought by the creator of the Auto-ID center at MIT. Auto-ID is used to identify many measures to improve applications, like work efficiency enhancement, automation, and error reduction. The Auto-ID center came up with the idea of electronic product codes (EPCs). EPCs allow for tracking things moving from one place to another. This was the birth of the internet of things as we know it. The idea that we could create a network for mainstream commercial means using microchips was real.

IoT technologies with vast application base across sectors, varied architectures and ever-changing developments cannot be contained with a simple definition. However, a report from the International Communication Union in 2005 contained a formal proposal defining the IoT which is widely accepted is stated below:

"The IoT was proposed as a collaboration of computing and sensor-based technologies, such as sensors, wireless networks, embedded systems, object identifiers and nanotechnologies. This combination enables the objects to be tagged, sensed and controlled over the networks" [140].

1.1 The Origin of the Internet of Things (IoT)

The IoT is the combination of technologies with a goal to provide communication and interaction between connected devices which can collect, process, analysis, report and take intelligent decisions. Many enterprise systems have been developed for healthcare, energy, vehicles, decision making, mining, education, smart cities, and more. Figure 1 below attempts to capture the sectors where IoT applications are actively researched and effectively deploy.

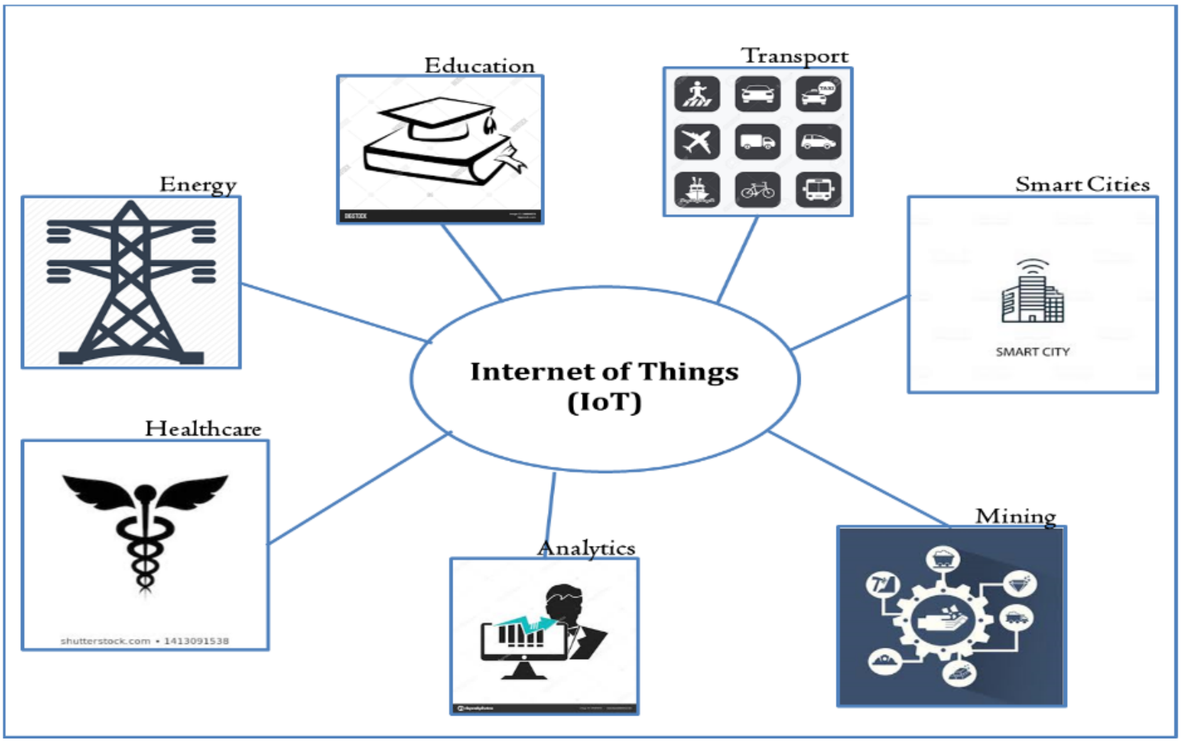


Figure 1. Sectors where IoT technologies have already made inroads

1.2.1 IoT in Health

One of the most important applications of IoT is Healthcare. Hardware such as sensors are either worn on the body or in the body itself which measures health parameters and which are transmitted through connecting networks to the databases, where the data is processed and stored. Cutting-edge algorithms can process and analysis the collected data efficiently and economically. If data is gathered correctly, continually, and effectively this information can lead to a huge positive transformation of the healthcare world, making it possible for the healthcare sector to move from a reactive diagnose and treat system to a more proactive and predictive medical practice model. This means earlier disease identification, prevention, cure, and better management of health. Healthcare solutions could no longer be a one size fits all solution, as they could be specifically tailored to the needs and circumstances of the individual.

Using this data as well as decision-support systems, the physician will have a much better idea of the current state of your health and in turn make better recommendations regarding treatment, intervention, or lifestyle choices. These IoT technologies are poised to transform global healthcare systems, reduce healthcare costs, and improve the speed and accuracy of disease diagnosis.

1.2.2 IoT in Vehicular Networks

Automotive industries have experienced unprecedented growth in the last decade, during which the number of vehicles reached approximately 900 million in 2006 [96]. This number broke through 1 billion in 2014 [104] and was predicted to reach 2 billion by 2035 [141]. Internet-of-Vehicles (IoV) a sub-set of IoT is enabling automotive solution providers to meet the challenges in the uprising complex traffic system and enhancing customer experiences with improved safety, time and energy efficiency, and productivity. IoV vision has inspired an automotive industrial revolution by moving from human-driving cars towards self-driving cars.

According to the IoV vision, Vehicles and devices share information based on five basic models, such as Vehicle to Vehicle (V2V), Vehicle and Roadside (V&R), Vehicle and Devices (V&D), Vehicle and Person (V&P) and Device to Device (D2D) [90]

All interconnected IoV end devices (e.g., vehicles other electronic devices) can not only exchange and process information locally but also to share information to IoV information platforms through different wireless access technologies (e.g., Cellular systems, Wi-Fi, WiMAX, and WAVE). The IoV information platform is capable of processing and computing all uploaded data and pro- viding a large variety of application service. In general, the IoV concept aims to improve drivers' sense of external traffic environment, achieve the optimal driving decisions, and minimize unwanted accidents caused by human factors [96].

1.2.3 Behaviors and Decision Making

Wireless IoT has been adopted effectively in monitoring and predicting behavior and decision making of people and animals. The systems are used to develop prediction models how people or animals will react to certain situations and detect patterns in their behavior. One of the main applications where behavior and decision making IoT systems are used in the tourism industry, where people's decision to visit certain attractions can be captured and prompt recommendations for other attractions which they may enjoy [93].

Patterns from the data collected from IoT systems are also used to design the tourism locations more efficiently based on foot traffic, time spent, etc. It provides required inputs to provide other infrastructure such as transportation, restaurants, and other outlets, which not only makes the tourist experience better, it also improves local businesses to plan more efficiently and increase their revenues. Advanced IoT systems can also be developed to personalize tourism and shopping experiences based on the behavioral and design making patterns.

1.2.4 IoT in Learning Environments

Even though schools and universities are the steppingstones for R&D efforts in developing cutting edge technologies, they have been slow in adapting and implementing them. IoT applications have made in-roads into all sectors but their penetration into education sector has been lagging. There have been some serious considerations lately to deploy IoT which has the potential to transform education sector. IoT combined with other technologies such as data analytics, AI, etc. is providing better learning experience for students through personalized and dynamic learning.

Smart learning environments with embedded sensors, actuators and other devices can create perfect synergy between physical and digital realities, allowing development of environments for better absorption of information, individual and group learning, online education, etc. The information collected can also be used by teachers understand how students are responding to the assignments and tests and to design better learning systems. IoT applications from other sectors are already in use in schools and universities, such as, temperature sensors to reduce the energy consumption, tracking systems to track school buses and to provide better parking solutions, wireless and intelligent networks to provide remote door locks, connect surveillance cameras and facial recognition systems, etc.

1.2.5 IoT in Mining

Mining is a vital sector which drives global economy, meeting the needs of the ever-growing population for minerals, fuel, and metals. According to IBISWorld US Report [3], mining in America is majorly employed in oil and gas extraction, coal mining, iron ore mining, gold and silver mining, mineral and phosphate mining, molybdenum and metal ore mining etc. With the advent of the Internet of Things (IoT), these mining industries are heavily relying on them for better exploration, extraction and trade. Sensor and network technologies bring the necessary features to record and communicate humongous amount of data that gets analyzed in real-time. These advancements give rise to multiple actionable insights for researchers and explorers to identify and develop commercially viable mines.

In mines, most of the sensor data comes from observation of environmental conditions. Hence, a specialized wireless sensor network (WSN) known as Wireless underground sensor networks (WUSNs) is deployed for monitoring). WUSNs help against fire monitoring [24], prevention against the collapse of unstable shafts, faulty equipment alert [97], productivity, the safety of mine workers, and reliant underground communication [9].

1.2.6 IoT in Energy Systems

A common term for IoT in Energy systems is the Internet of Energy (IoE). Over the next 25 years, energy usage is expected to increase by over 40%, making the need for smarter energy solutions at an all-time high [12]. Many different devices around the household are becoming smart energy devices; from things like smart meters down to even smart light bulbs. IBM predicts that by 2020 there is a possibility of 925 million smart meters, 2.54 million smart lights and 1.53 billion utility-managed connected devices [136] IoT in energy systems is not just being used for consumers, but different companies in all types of industries. Companies, such as GE, are using IoT to monitor energy usage and help plan preventative maintenance schedules based on different analytics [12].

Numerous IoE solutions are evolving across energy sector revolutionizing the way energy is generated, distributed and consumed. In generation it is extensively deployed in renewable (green) energy industry. In windmills IoE devices continuously monitor wind, temperature and other environmental data, analyze most productive and efficient setting, and automatically adjust wind turbine directions for maximum energy production. Similarly, applications are developed for solar fields, geothermal plants, and traditional oil and gas for enabling more efficient energy production, better safety, and more importantly to predict major plant breakdowns and initiate preventive maintenance [52]. In energy distribution IoT solutions are combined with drones to provide real time data on transmission networks, predict any leakages, etc. For consumers, IoT sensors installed in homes and offices sense the environmental parameters real time, analyze real time and historical data and adjust home equipment such as HVAC systems, lighting, etc. for efficient use of energy and to reduces energy costs [52] For example, Tipmont REMC, the local power provider in Tippecanoe county, uses smart meters that provides customers real-time information on energy utilization which helps them to take conscious decisions on their energy consumptions.

IoE is also providing solutions to develop smart grids which reduce dependency on large centralized generators bring generation closer to the consumption thereby reducing transmission losses. The smart grids equipped with IoE devices can completely transform how energy will be distributed and stored [103]. Blockchain technologies is also integrated with IoE to develop platforms to trade energy securely on energy markets, making even peer-to-peer trading a possibility.

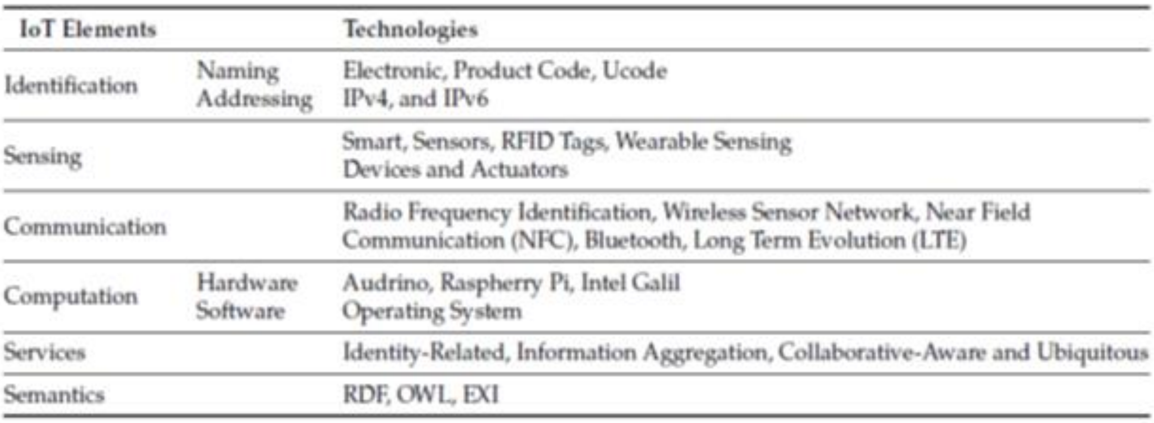
1.2.7 IoT in Smart Cities

Smart cities are another area where IOT technology is being used to improve the lives of its denizens. IOT technology can fit into many different places of a city's operation, ranging from transportation, environment monitoring, accessibility and healthcare, to waste management [98]. The possibilities of IOT technology to improve lives, interconnectivity, and information sharing allows cities to more easily and efficiently manage resources, such as conserving energy from lighting, or even law enforcement by tracking suspect vehicles with a UAV network. However, despite the many technologies that are being developed for smart cities, there is yet an agreed upon definition for what constitutes a smart city [58]. Smart cities can be generally characterized by incorporating 6 factors: economy, mobility, environment, people, living, and governance [23]. Examples of smart city technologies that would fall into these categories include simplified payment systems, smart public bus routing, smart power grid, and smart homes.

One potential main driving force for the push to develop smart city technology lie in the fact that urban populations have increased drastically with the rapid increase of global urban population from approximately 1 billion in 1960; 2 billion in 1986, 3.2 billion in 2005 and an estimated 5 billion in 2030 [23]. Cities with "Smart" tag with IoT networks and solutions not only provide best living conditions to its denizens but also receive additional funding, making more and more cities to jump on to smart city bandwagon [70].

2. Architecture

IoT technologies having the potential to revolutionize the way all things are developed in the coming years, several companies, organizations and countries are working on multiple solutions and applications across all sectors. Like any new technology IoT is also currently going through the stage where there is no single architecture or standard. Few models are already found to be most accepted by the industries which are presented here. The underlying technologies are already standardized and have been around for some time and have been listed in the table below.



IoT Elements		Technologies
Identification	Naming Addressing	Electronic, Product Code, Ucode IPv4, and IPv6
Sensing		Smart, Sensors, RFID Tags, Wearable Sensing Devices and Actuators
Communication		Radio Frequency Identification, Wireless Sensor Network, Near Field Communication (NFC), Bluetooth, Long Term Evolution (LTE)
Computation	Hardware Software	Audrino, Raspherry Pi, Intel Galil Operating System
Services		Identity-Related, Information Aggregation, Collaborative-Aware and Ubiquitous
Semantics		RDF, OWL, EXI

Table 1. The elements and key technologies of IoT (Burhan, 2018)

The main functions IoT architecture should cover are sensing and collecting data, communication network to transfer data to the cloud or processing center, and data processing involving analytics, visualization, etc. Based on the complexity of the application and the level of security required different models are adopted, of which the popular models based on the number of layers are Three, Four and Five Layer architecture [117].

doi:10.20944/preprints201912.0276.v1

1. Three Layer Architecture is a basic model on which simple IoT solutions can be developed [71]. It has perception, network and application layers to collect, transmit and process data. However, this simple model lacks the ability to provide high reliability and security required in the healthcare sector.

2. Four Layer Architecture is proposed by researchers by adding an additional Support Layer which provides security mechanisms to safeguard the system from potential attackers [46]. This particular model suffices the needs of most industrial applications and quite frequently adopted.

3. Five Layer Architecture is introduced to take care of ever-increasing quantum of data, complexity of information sought, and the integration of multiple services on a single platform [121]. It adds two layers namely, processing layer and business layer. Processing layer screens the data collected and extract important information thereby reducing the load on the system. As more and more services are added to the applications Business layer manages these processes and the system as a whole.

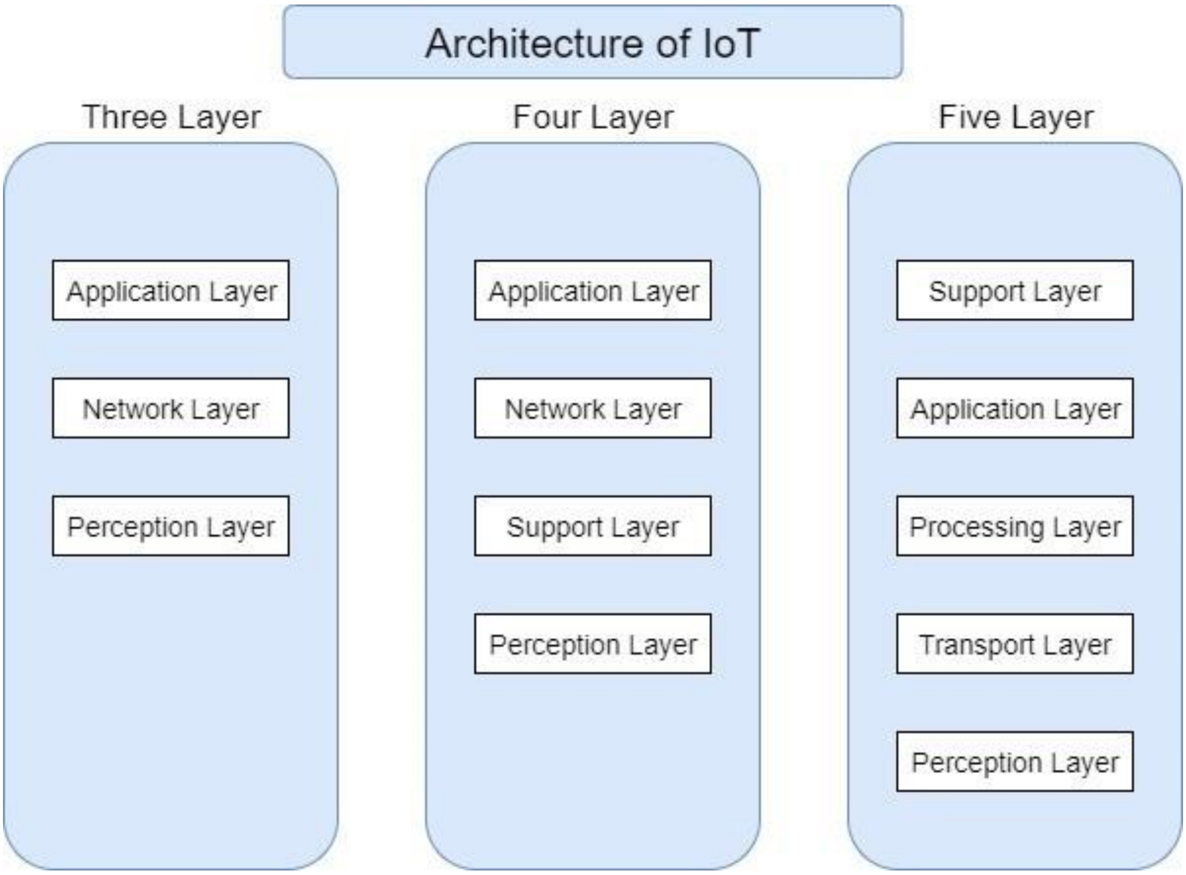


Figure 2. The layered architectures of IoT (three, four and five layers)

The layers in each of these models are combination of: Perception layer, Network layer, Application layer, Support Layer, Transport Layer, Processing Layer and Business Layer. A more detailed explanation of the layers is given below.

Perception Layer:

The perception layer is also known as the sensor or recognition layer. It is the lowest layer of architecture in IoT which is connected to the subject under observation. This layer collects information from the environment such as location, vibration, moment, humidity, temperature, medical parameters (in case of healthcare applications), etc. It is a physical layer and it uses sensors such as RFID, sensors, Bluetooth, Near-Field Communication and 2-D barcode. A good example of sensors that are used every day are the smartphone and fitness gadgets. This layer is the major differentiator from vertical to vertical, whereas other layers share technologies as they have several commonalities.

However, the perception layer is most prone to security threats as it is the weakest in security protocols. The common threats are [82] for this layer are listed below, and the devices developed for this layer should address these threats by adopting appropriate measure to counter the weaknesses.

a. Eavesdropping: It is also known as sniffing or snooping attack. It occurs when attackers try to steal information through smartphones and computers or other devices that are part of an unsecure network. They are difficult to detect as they do not interfere with the regular transmissions.

b. Node Capture: Through this an attacker can interfere with various operations and compromise the entire network. The attacker gets complete control over the key node such as the gateway node and can leak data communicated through this network. Access to the nodes not only gives the attacker knowledge about the existing network information but also lets them deploy malicious nodes into the network.

c. Replay Attacks: These types of attacks are also known as play back attacks. An attacker may eavesdrop on the transmission and then have the transmission either delayed or repeated. It is hard to detect this attack as the message is encrypted and the receiver may presume it to be an authentic request and respond to attackers' commands.

d. Timing Attack: The attacker tries to compromise the network by understanding the network and keeping track of the time it takes the system to respond to different inputs and queries. Timing of a system depends on the encryption key and is different for different systems. The attacker uses statistical analysis to understand the key and gets access to confidential data.

Network Layer:

This layer is also known as the transmission layer. It is the brain of the architecture of IoT and is used to transmit data between the application and perception layer. This data can be transferred using various technologies like wired, wireless and satellite. Because of tremendous advances made in communication technology this layer is the most developed layer of the architecture. As this layer deals with the transmission of data with the longest physical link, it is highly sensitive to security threats and network problems. Network layer provider should implement this layer with necessary safeguards against below attacks.

a. Denial of Service Attack (DoS): In this attack the intruder prevents the user from using the machine resource by flooding the network with inputs and queries which makes it hard for other users to use it. The high traffic makes the system to initially slow down and then eventually stop.

b. Main-in-The-Middle (MiTM) Attack: The attacker eavesdrops into the communication and alters the communication amongst the users. The attacker not only gets access to the information that is being relayed but also can change the information that is being transferred. This threat is hard to detect as the users will not the intermediate leakage and corruption of info by the attacker as they presume that the communication is direct between the sender and receiver.

c. Storage Attack: Most of the information of the users is stored in devices or the cloud. An attacker can gain access to these storage devices and gain access to the information. The users' information gets leaked and often duplicated and used by attackers maliciously for wrong purposes.

Application Layer:

The application layer is the top user layer through which the IoT application directly interacts with the end users. The IoT systems can be smart homes, smart cities, smart health, etc. This layer is responsible for providing services at the application level by adopting appropriate protocols such as CoAP, MQTT, AMQT, XMPP, RESTFUL, Websockets, etc. and to provide a medium for IoT to be deployed [20]. The following are examples of security threat that this layer may face and therefore should adopt appropriate protocols.

a. Cross Site Scripting: These types of attacks are also known as injection attacks as the attackers inject a malicious script such as java script into the existing script. This lets them gain control of the application giving him access to change the information to his personal advantage or to harm the user.

b. Dealing with Mass Data: This layer usually has large traffic of data and hence may lead to problems during data processing. This could lead to data loss or cause the network to crash due to the excess data flooding.

c. Malicious code attack: These types of attacks extremely difficult to address as most anti-virus software tools cannot block it. It is a malicious attack intended to damage the system by injecting bad code at any weak link in the application.

Support Layer:

The support layer was introduced in the four layered architecture of IoT. It is placed between the application and network layers in order to reduce the threats that were caused by sending information directly to the network layer. The support layer needs to authenticate the information sent to it and then transfer the data to the network layer. However, there is still scope for some of the attacks listed below to take place in this layer which need to be properly addressed.

a. DoS Attack: As mentioned above, the attacker sends a flood of input into the network layer in order to create high traffic preventing authenticated users from accessing it.

b. Malicious insider attack: These types of attacks are hard to stop as they usually originate from inside the network to gain personal information about other users.

Transport Layer:

This layer is also known as transmission layer introduced in the five-layer architecture model for IoT. The main role of this layer is to transfer the information from the perception layer to the processing layer. It provides end-to-end communication in the network. Based on the requirements it uses communication technologies like Home Area Network (HAN), Field Area Network (FAN) and Wide Area Network (WAN) to fulfill the needs.

Processing Layer:

This layer is also known as middleware layer process the information and transfers it to the transport layer. Middleware is used to provide a unified production model for the devices to interact by connecting already existing programs and creating a bridge between the perception layer and the application layer. It reduces the bottlenecks that are caused by big data as it removes the excess information which is not useful for the system. Some of the common attacks that processing layer faces are:

a. Exhaustion: Attackers flood the system with excess data and indefinite queries through a DoS attack which leads to exhaustion of the system due to the overuse of the systems battery and memory. This attach is intended to disrupt the IoT processing. However, as IoT has a distributed architecture it is easier to prevent such attacks.

b. Malware Attacks: Malware attacks are introduced through viruses, spyware, adware, Trojan horses and worms to steal confidential personal information. These occur without the knowledge of the user through codes and scripts and hence are hard to detect.

Business Layer:

The business layer works as the manager for the entire system. It is the topmost layer of the five-stage architecture model for IoT. This layer is also responsible for managing the user's privacy. It is required to collect data from all the other layers and create a digitized version of the combined data. It also decides how the data will be collected, used and stored. The threats that are usually faced by this layer are because of lack of security and disregard of the business logic by the attackers. Some of the common attacks are:

Business Logic Attack: These attacks take advantage of the defects in the system such as poor coding, input validation and encryption techniques. This attack can take control over the information that is being transmitted between the users and database.

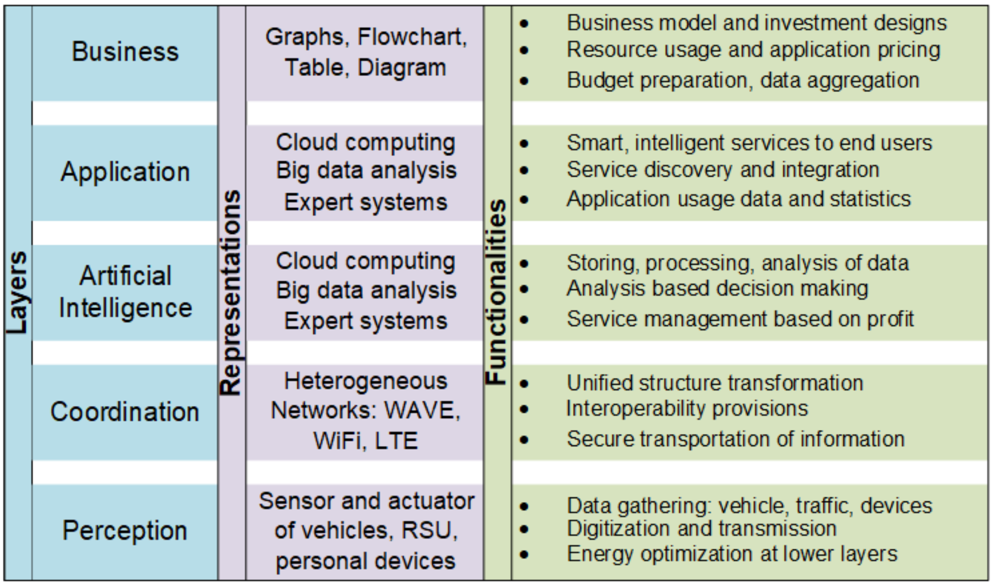
Zero-Day Attack: This attack exploits the existing security hole in the system to gain access to user's confidential information and transactions.

IoT in Vehicular Networks

This section presents and reviews several currently existed IoV architectures. In IoV research field, the most challenging topic is to tackle communication issues in different applications, such as traffic control, vehicle health monitoring, safety, and infotainment. Collecting data from a large quantity of deployed sensors further imposes challenges to the implementation of the local network in a vehicle. Consequently, these applications demonstrate limitations in interoperability due to information security, accessibility, interference, and availability. Several attempts have been proposed to increase interoperability and to develop multi-platform architectures which enhance interactions between hardware objects (e.g., vehicles and devices) in an IoV environment [135]; [89]; [141]; [78]; [43].

Liu [89] proposed an IoV architecture based on three layers: client, connection, and cloud as illustrated in figure 3. As for the client layer, all internal and external sensing end devices are used to collect information, such as acceleration, speed, relative position, tire pressure, oil level, road obstacle, and vehicle health conditions. The connection layer secures inter- operability among all supported networks in which no signal interference, data latency, and data redundancy occur. All collected data eventually travels to information platforms (e.g., cloud). The IT platforms provide a variety of applications and services to meet all requirements, such as data storage, information analysis, and decision making.

In Bonomi [30], the author presents a four-layer based architecture for IoV, as shown in figure 4. The first layer defines the V2V communication scenario in which the 802.11p protocol is proposed to establish links between vehicles. The second layer, referred to infrastructure, includes all enabling technologies (e.g.) which connect all hardware objects in the IoV system. The third layer, operation layer, supervises the operation of IoV system to ensure compliance with all existed polices. The last layer (e.g., cloud layer) characterizes different cloud services (e.g., public, private, and business) and accesses to these services according to different requests (e.g., voice messages, entertainment video, and other types of data).



Layers	Representations	Functionalities
Business	Graphs, Flowchart, Table, Diagram	• Business model and investment designs • Resource usage and application pricing • Budget preparation, data aggregation
Application	Cloud computing Big data analysis Expert systems	• Smart, intelligent services to end users • Service discovery and integration • Application usage data and statistics
Artificial Intelligence	Cloud computing Big data analysis Expert systems	• Storing, processing, analysis of data • Analysis based decision making • Service management based on profit
Coordination	Heterogeneous Networks: WAVE, WiFi, LTE	• Unified structure transformation • Interoperability provisions • Secure transportation of information
Perception	Sensor and actuator of vehicles, RSU, personal devices	• Data gathering: vehicle, traffic, devices • Digitization and transmission • Energy optimization at lower layers

Figure 3. A five-layered IoV architecture

Kaiwartya et al. [78] describes a five-layer architecture which contains perception, coordination, artificial intelligence, application, and business. The first layer (e.g., perception) includes all types of hardware devices. These devices collect internal and external information in forms of vehicle health, road condition, traffic and status of other electronics devices (e.g., cellphones, tablets, and wearable electronics). The coordination layer aims to implement a networking coordination module and ensures uploading data safely to cloud services. ices. The cloud infrastructures stores, computes, and analyzes the information from the networking layer and makes decisions according to clients' requests and applications. The business layer processes data using different statistical tools. The data, in the form of graphs, charts, and tables, helps to generate business strategies.

To further clarify and simplify functionalities of each layer and standardize protocols, Contreras-Castillo, Zeadally, and Ibanez [43] proposed a seven-layer architecture which comprises user interaction, acquisition, pre- processing, communication, management, business, and security. The inter- action layer aims to design friendly user interfaces for a vehicular internal operating system. The challenges arise in improving user experiences without much interference with driving performances. The data acquisition layer collects data, representing safety, traffic, infotainment, from existed sensors, electronic devices, and actuators. Several works have been carried out to propose data collection schemes based on road division [32]; [38]; [105]. Several other works focused on data collection based on the vehicle's mobility and network topology [69]; [126]. The author in this paper defined data collection scheme into two categories: intra vehicular interaction and inter-vehicular interaction. The data filtering and pre-processing layer aim to filter out junk data which introduces irrelevant information and network traffic. Several data mining-based filtering techniques have been reviewed in this article [57]; [61]; [108]. The communication layer utilizes different wireless networking technologies to create a heterogeneous communication environment. This layer targets to provide full connectivity and truly seamless services to every single end-user with available access wireless technologies (e.g., Bluetooth, ZigBee, Wi-Fi, and Ultra-wideband R8F). The proposed layer also described potential network candidates, such as SAW, TOPSIS, MEW, GRA, and VIKOR. The control and management layer are responsible for managing both information generated from the data acquisition layer and network services in the communication layer. Accordingly, policies will be made to improve multiple tasks in traffic management, data packet inspection, and traffic engineering.

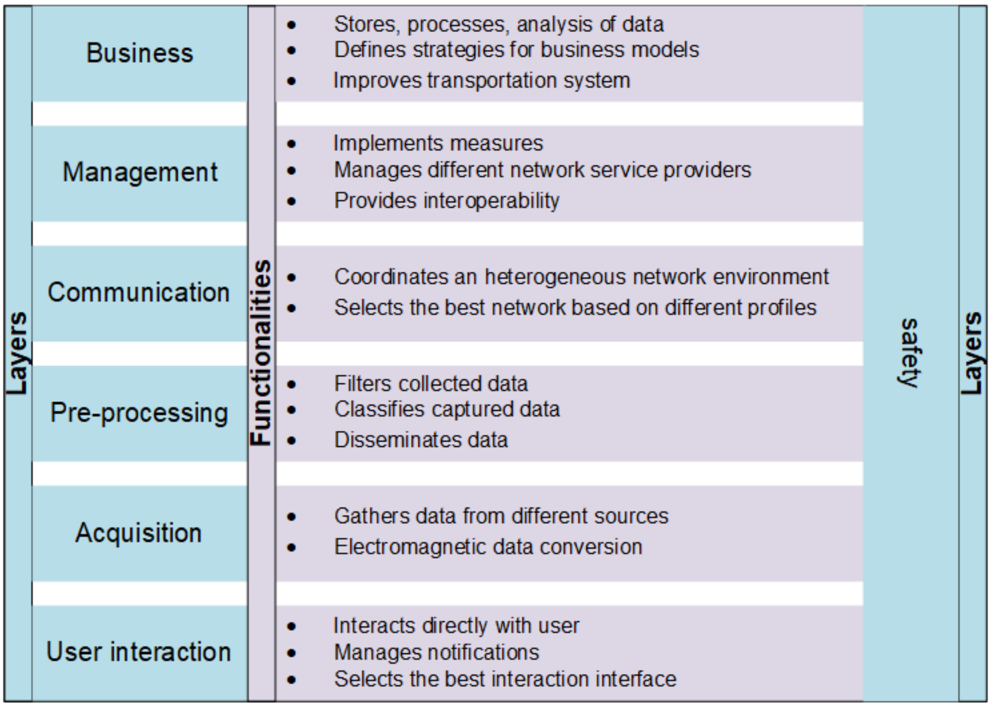

Layers
Business
Management
Communication
Pre-processing
Acquisition
User interaction
Functionalities
Stores, processes, analysis of data
Defines strategies for business models
Improves transportation system
Implements measures
Manages different network service providers
Provides interoperability
Coordinates an heterogeneous network environment
Selects the best network based on different profiles
Filters collected data
Classifies captured data
Disseminates data
Gathers data from different sources
Electromagnetic data conversion
Interacts directly with user
Manages notifications
Selects the best interaction interface
safety
Layers

Figure 4. A seven-layered IoV architecture

The business layer processes a large quantity of data using various remote and local cloud computing platforms and generates analytically statistical data (e.g., graphs, flowcharts, and tables) which can be used for further development and improvement of IoV system infrastructures and other ser- vices. The security layer supervises all other layers in a security perspective and prevents the IoV infrastructures from different types of security attacks (e.g., cyberattacks).

Behaviors and Decision Making

The architecture for an IoT topology with the capability to monitor behaviors can be built in multiple ways and using various techniques. As explained in [17], there are two main groups of techniques: those that are not based on Wi-Fi tracking and those that are. In the context of this piece, only Wi-Fi based techniques will be discussed. Other techniques use technologies such as radiofrequency (RF) measurements, GPS location data, Pedestrian Dead Reckoning (PDR), and Bluetooth to track people and their behaviors in public areas. Each of these alternatives to using Wi-Fi come with some limitations that make monitoring behaviors less feasible in some way. Using Wi-Fi to monitor is easier and able to provide more useful data since the MAC addresses can be collected and used as a means of identifying individual users and creating unique profiles for each one. This is exactly how the data is collected in [17] is the architectural paradigm from which this paper is approaching behavioral monitoring. Monitoring using Wi-Fi is typically done by two different methods. The first method is to use an already existing WLAN. Although this would keep the cost of the system low, it should be noted that this will only allow users connected to the specific WLAN to be monitored. The second method is to install a low-cost passive sniffing infrastructure. This dedicated solution can monitor activity from multiple Wi-Fi networks and collect the same data about all the users. Only a few very simple tools are necessary to implement sensing which will be discussed further in section four of this paper, but to briefly touch on them for now, they are: A Raspberry Pi, a TP-LINK USB Wi-Fi dongle, and a developed Wi-Fi listening device. These tools working in unison help to automate the data capturing process and also keep costs down. A different approach would be appropriate if a different type of behavior is being monitored. In [99], the behavior being analyzed is to be used for health purposes so that changes may be made to a patient's care or action may be taken in case of an emergency. Sensors that monitored behavior regarding the subjects is drastically more specialized. These devices/sensors will be covered in more detail in section.

The sensing portion of these architectures act as the interface by which information is gathered. The information then must be transmitted through the IP network utilizing the appropriate protocols. The data is eventually routed to a backend server where various processes take place on various systems. These systems will be discussed in greater detail in section 5. End-to-end protection is provided by Transport Layer Security (TLS) over TCP/IP protocol and Message Queue Telemetry Transport (MQTT) sends periodic measurements by using the publish/subscribe mechanism. The MQTT is a protocol that, according to [99], relies on a broker to send and receive data between subscribers and publishers. With this configuration, Wi-Fi enabled sensors can send measurements and receive commands over SSH sessions. In the scenario provided by [17], privacy of the data sent across the architecture has been covered by having the Wi-Fi sensors use an MD-5 hash function and salting the MAC addresses. Figure 10 provides a visual illustration of the architecture used in [17] and the direction of data flow starting at the sensors, through UPM IP network and directly into the

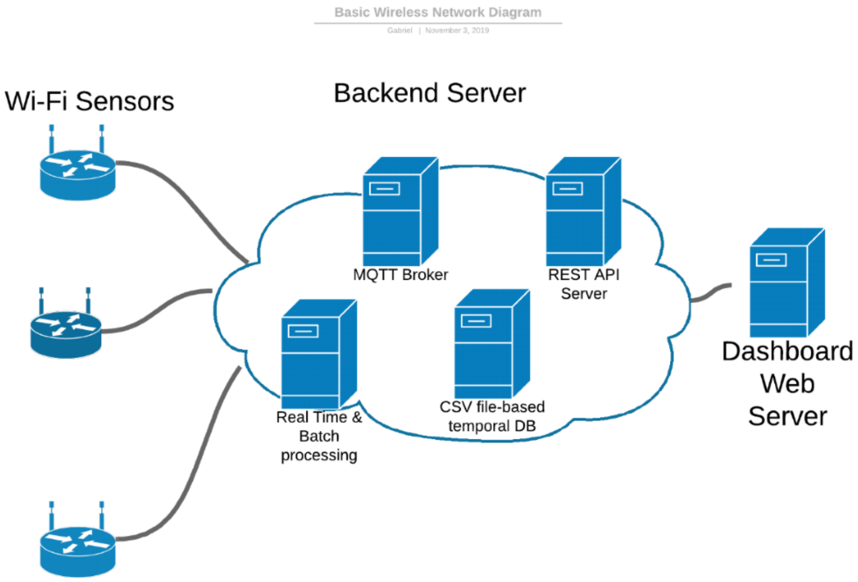

Basic Wireless Network Diagram
Gabriel | November 3, 2019
Wi-Fi Sensors
Backend Server
MQTT Broker
REST API Server
Real Time & Batch processing
CSV file-based temporal DB
Dashboard Web Server

Figure 5. The architecture implemented in (Andion, Navarro, Lopez, 2018) to monitor and process behavioral data of students at UPM

backend services. The figure also depicts the protocol stack through which the traffic has been configured to flow.

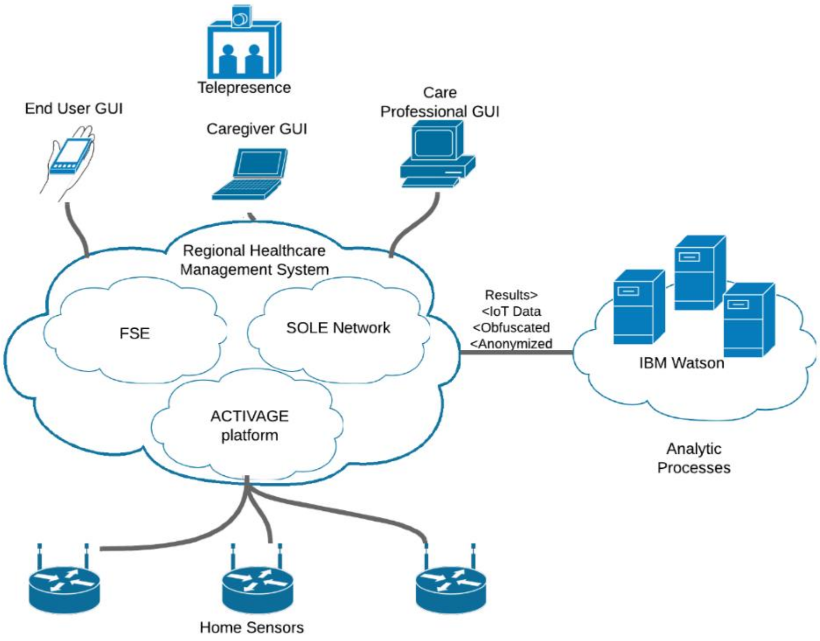


Figure 6. The architecture implemented in (Mora, Grossi, Russo, Barsocchi, Hu, Brunschwiler, Ciampolini, 2019) to monitor and process behavioral data of patients at home

Figure 11 below shows the architecture deployed in [99] used to sense, collect, and process health behaviors throughout a home and present that information to caregivers. It interfaces with IBM Watson for data processing in the cloud. The use of cloud computing ensures that the system can be scaled in the future and that it is highly available.

Many aspects of these two architectures are essentially the same. Except that their specific hardware is appropriate to the type of monitoring needed, processing is fulfilled by different service providers. One additional difference is that the architecture in Figure 2 also provides GUIs to individuals who would require access to the information being collected. This includes the end user who is being monitored, a caregiver who could be watching over the end user and a healthcare professional. The interface used by the caregiver is the SOLE network which is the network that the architecture is built around. The end-user GUI is FSE (Fascicolo Sanitario Elettronico) and interfaces directly to Electronics Health Record System. ACTIVEAGE is the formal name of the platform built to interface with the IoT devices setup in patients' homes. It is a part of the Regional Healthcare Management System and interacts directly with SOLE network and the FSE platform. Since the data being collected is eventually related to personally identifiable health information, the architecture must be considerate of security vulnerabilities. For this reason, the sensors are set to only be able to publish data to the ACTIVAGE platform, but they are not able to pull down any data. A REST-API is also in place which is used to allow subscribers to get the data they need and ensures that users are not directly accessing the database.

There are other ways in which behavioral data can be useful besides in health care and in monitoring traffic throughout a college campus. In the Roman Department of the Allard Pierson Museum of Archaeology in Amsterdam, The Netherlands, IoT devices are used today to monitor the behaviors of museumgoers. The data is then used to recommend different paths through the museums exhibits within the department based on decisions made by past visitors. This architecture is fitted with sensors inside the museums Points-of-Interest (POI's). These sensors collect data pertaining to users' actions once they arrive at any POI by telling the user to scan an RFID chip card. The behaviors that the user engages in can then be associated with their specific RFID chip so that the path they took through the museum is recorded but also the way they interacted with each exhibit. In this kind of architecture, the aim is "to model users information interaction behavior with IoT having an aim of providing a personalized onsite POI recommendation".

Something that is especially unique about this architecture is that it not only gathers data based on onsite physical behavior but also online digital behavior. According to [55], this onsite data collected performed even better than onsite as a predictive model for learning visitors' actions. In [55], 3 different metrics, mean reciprocal-rank (MRR), mean average precision (MAP) and R-precision) are used to measure the effectiveness of different types of users' interactions behavior in understanding their onsite preferences. On all three metrics, online behavior performed the best at collecting the predictive information of visitors accurately enough to have the most impact than onsite. The online behavioral data is sourced from search engine query logs. Although the researchers in [55], have found that online data performs better vs the onsite data, they also found that when the architecture collects and combines onsite and online data for learning a model it performs better than either method when used alone.

The aggregation of both types of data drastically increases the performance as opposed to solely using onsite data because understanding the prediction of users' onsite behavior can be challenging due to different users exhibiting different onsite behaviors. Users simply take different paths throughout the museum. These challenges will be discussed in further detail in the challenges section. Aside from the challenges though, it is a highly accurate form of detecting specific but completely normal activity without even being noticed.

In our modern society, the use of technology for the purpose of making human life more comfortable and stress free is commonplace. Many features on smartphones today are designed around the convenience of their functionality compared to the previously used alternative to complete whatever task they require. In [31], a very complex architecture is used to capture data pertaining to the activities and behaviors of people living in a house. In the paper titled A Framework for Creating Personalized Smart Environments Using Wireless Sensor Networks, the architecture is comprised of various wireless sensors that gather information to later be used in making decisions to better serve the inhabitants of the environment. The sensors themselves, which will be discussed more in the sensing section, are separated into wireless sensor networks that serve different purposes

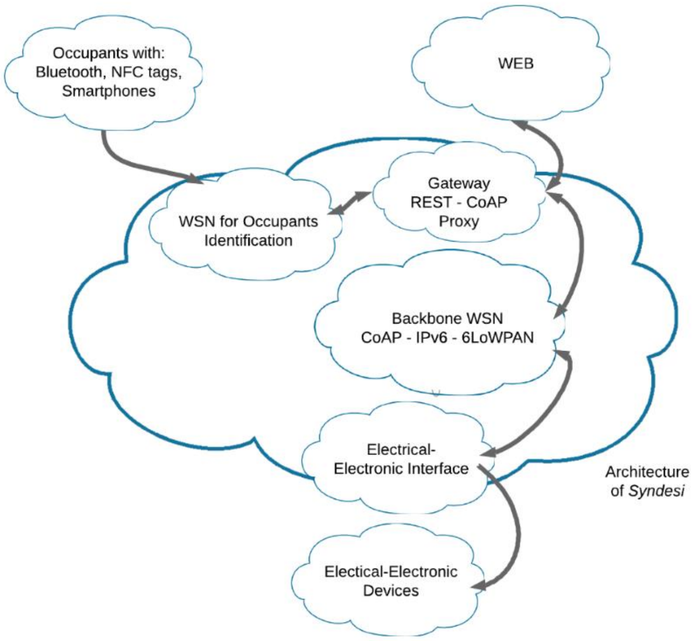


Figure 7. The Syndesi Architecture from (Evangelatos, Samarasinghe, Rolim, 2013) used to control devices based on readings taken by the WSN

doi:10.20944/preprints201912.0276.v1

and are of various types thus the architecture calls for technology that can integrate them all seamlessly. The architecture contains 2 separate Wireless Sensor Networks (WSNs) that interface with the gateway. One of the WSNs is for identification of users within the environment as well as tracking them and the other is the backbone WSN containing sensors that take care of analyzing and controlling the rest of the architecture and some of its environment. On the gateway there are connections to both WSNs and to the Internet. It also houses a proxy server making the whole architecture web accessible. Connected to the backbone WSN is an electrical/electronic interface that transmits output to electronic devices and electrical appliances ultimately controlled by the environment, that triggers the sensors in the backbone. The architecture is illustrated here:

The implementation of Internet of Things (IoT) devices are increasing all over the world in many aspects from reserving energy to providing safer transportation systems. In order to prepare for the future generation to adapt and be ready for the usage of IoT technologies, Internet of Things systems should be installed in educational institutions and schools to assist students and teachers to improve the quality of teaching and learning process and raise the awareness of its applications. The Internet of Things devices can be applied anywhere on campus and they can connect everyone and everything together.

A. *Internet of Things architecture*

The architecture of the Internet of Things has three layers: application layer, network layer, and perception layer [88].

Application layer

Application layer is the top layer of the Internet of Things architecture and it is also called "transmission layer". The main purpose of this layer is to supply large services such as smart cities, smart cars, and smart homes [88].

In some models, the application layer is divided into three different layers including middleware layer, application layer, and business layer. When this layer is broken down into three smaller layers, the middleware helps to ensure every device only contacts with others within the same type of service. Information will be stored and processed in the database for service management and making decisions. The application layer still indicates the big picture of smart applications and smart systems while business layer oversees providing the entire Internet of Things management system with business models, graphs, flowcharts to visualize and develop the systems depending on the current information [79].

Since Internet of Things system connects many devices together, it helps to utilize many resources to provide better, more efficient, newer features and functions that people never get to have before. This is the reason which requires appropriate business models and decisions to take advantage of the advanced technologies.

Network layer

Network layer is the middle layer of the Internet of Things architecture. This is also known as the "transmission layer" [79]. Transmission or network layer is a very important layer because they are the transporter for information. There are many network equipment, protocols, and communication technologies which are implemented to send information from the accurate sources in perception layer with sensors to the accurate destinations in application layer (middle layer) and vice versa. Network layer can send data and information through wired or wireless communications with different technologies such as GPRS/EDGE, UMTS/3G, 4G/LTE, 5G, Bluetooth, ZigBee, Wi-Fi 802.11 a/b/g/n/ac, Wi-Fi 6 (802.11ax), RFID, infrared and more [88].

Perception layer

This layer is the bottom layer of the Internet of Things architecture and it is also called "device layer" because it includes sensors, physical devices and objects [79]. Perception layers helps to create connections between devices and put them in the Internet of Things architecture. The information from these devices will be collected, processed, and sent to upper layers for other purposes. Sensors can collect lots of pieces of information from motion, vibration, humidity, chemical changes, temperature, location, etc. by using RFID, infrared sensor, temperature sensor, pressure sensor, proximity sensor, accelerometer and gyroscope sensor, optical sensor, smoke sensor, and etc. [88]. For example, an Internet of Things system in learning environment such as a university campus or a school can apply motion detector sensors for light switches so that when no one is in the room and no motion is detected, the lights will turn off themselves off to save energy. If there is someone in the room and the sensor can detect its motion, the lights will be turned on automatically.

With the general Internet of Things architecture described above, many architectures can be applied and combined to create a smarter infrastructure and system. This will bring about a smarter school/university and a smarter learning environment.

B. Internet of Things architecture in different area

IoT in Learning Environments

Student ID

Smarter student ID is getting more popular at universities and school system because of its convenience, reliable, and user-friendliness [26]. Traditional student ID card with a picture of the student and its student identification number helps to identify the identity of the person when it comes to any institutional tasks that require identity check. However, this is limited to human subjective view and usage. With the application of smart student ID by using RFID chipset, NFC chipset, or implementation inside smartphone and smartwatch, students can interconnect with many systems from transportation service, dining and dorm service to gaining access for buildings, labs, and school equipment with just a simple swipe or tap.

Many integrated technologies also come with smarter student ID such as attendance system using NFC or RFID Technologies [40]. Attendance is not only important at work, but it is also crucial at schools and universities. The attendance system or real-time visualization monitoring in-class activities, attendance and performance system firstly can keep track the attendance records of the students for administration purposes. This can also record student's involvement and interests so that the professors/teachers can improve and alter the interaction and study materials to improve learning outcome [147]. There are further applications by using smarter student ID such as registering for examination dates, payments, and many services on campus [28].

The student IDs can also be used to give access to printers, scanners, photocopy machines, and resources. This practice gains better security to avoid thieves, prevent unexpected, unauthorized, and unauthenticated parties to have access to the schools and universities' resources. Buildings access is another aspect that another layer of door and electronic security authentication method through smarter student ID can supply. Many devices and research labs contain expensive equipment, dangerous materials such as radioactive materials and dangerous chemicals; therefore, better restrictions are needed. Physical security in learning environment is fundamental practice in order to provide a positive and safe community to students, researchers, professors, and other facilities.

Surveillance security cameras

Closed circuit television (CCTV) is the video security surveillance which uses cameras to record and send the video signals to be watched in real time in an operation center or the video can also be saved in database for investigation or future usages if needed. The use of CCTV is to prevent crime, traffic and weather monitor, crime solving, etc. These systems can apply different technologies from wired- connection to wireless-connection to provide the service. With many advantages, CCTV in schools and learning institutions are increasing in the recent years around the world [22]. Cameras are installed in hallways, public places such as cafeterias, dining courts, lobbies, open study spaces, classrooms, etc. to prevent crime, violence, and improve school security. This system can contribute to the security and safety aspect of a smart campus or a smart learning environment concept when the police or security department can have an overview in different areas.

Lighting and A/C thermostat

Learning environment can also be affected by other characteristics such as lighting, room temperature, and air quality including carbon dioxide level, pressure, and humidity [131]. The application of Internet of Things through sensors can help to control the lights, thermostats, and detect air quality for classrooms and buildings. A central operation center or system can control and monitor the information from the sensors to decide the proper actions which help to save energy, resources and money [132]. Schools and institutions can apply this Internet of Things technology to improve the effectiveness of energy control management. Also, people are staying indoors more than outdoors such as offices, schools, restaurants, hospitals, libraries, bars, clubs, and homes. Indoor pollution has a bigger exposed rate to common people than outdoor pollution which causes asthma and cardiopulmonary pathologies [48]. Having the air quality tracking system, the proper thermostat system, and the air distribution system in schools with the assistance of Internet of Things will bring a better learning environment.

Smart classroom

Classroom is the place where everyone comes to learn. Traditional classroom with a blackboard, chalk, tables and chairs is the basic model for centuries. Students with different studying styles and professors with different teaching styles sometimes do not match up and it affects the results significantly. However, with the fast growing of technology these days, the classroom becomes more diverse and interactive in many dimensions. Smart classroom, smart school, or Internet of Things in learning environment can help to increase the interaction and engagement between teachers and students to improve the learning experience and learning result [147]. Many Internet of Things systems such as real-time automatic feedback or activity monitoring and visualization system are being tested and applied.

Yusof, Qazi and Inayat were researching the effectiveness of a system which checks the attendance, involvement rate, and interaction rate to demonstrate the students' attentiveness to assist teachers, professors, and administrative to alter teaching methods and build better connections with

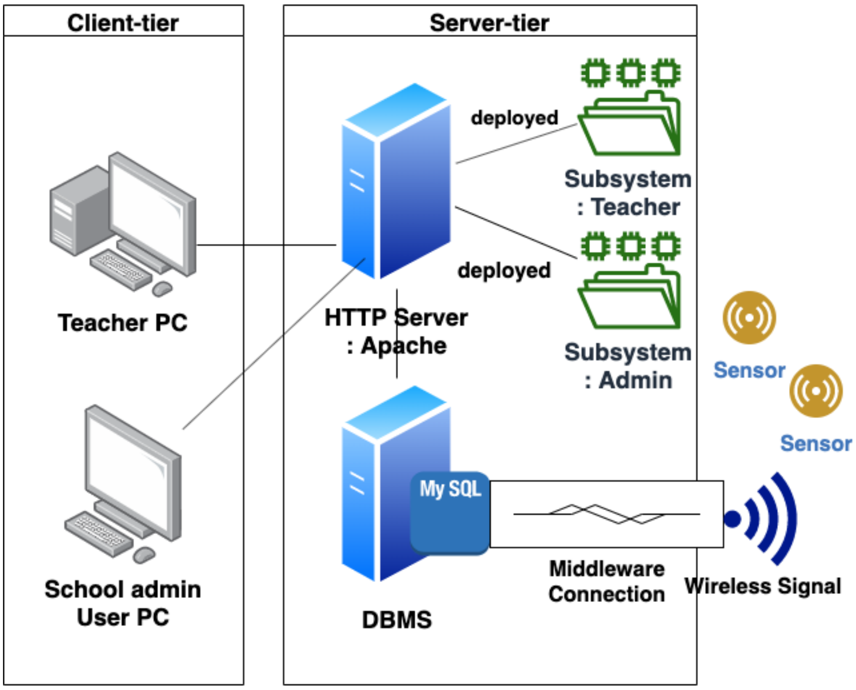


Figure 8. RFID-based real-tim e student visualization [147]

students. Figure 13 is a graph of student real-time visualization system (SRTVS) that the researchers are using. The system they use includes client-tier (desktops) and server-tier (Apache servers and MySQL). The network layer mainly uses RFID technology to connect with students to the system. Professors can update student profiles, attendances, exam grades, and involvement information [147].

Another group of researchers want to turn the classroom to be more active by proposing many more systems to be implemented in the classroom [131]. They mention a system that actively listens to movements and behaviors to provide feedback to lecturers and professors by using sound recorders, video recorders, motion detections (PIR sensor) to measure motion and noise existence and level. These pieces of information can combine with smartboards and smart wristbands to enhance and boost the interaction. Temker, Gupte, and Kalgaonkar state that the professor can use the vibration mode on the student band to catch the attention of the students and use the smartboard to display images, videos, and interaction assignments to connect students together.

Many IoT applications allow the interconnection between devices to transmit information across platforms [66]. This can combine many proposed systems to establish a smarter learning environment to benefit learning experience.

IoT in Mining

Two architecture are discussed in this section. One for surface mines and another for underground mines. The underground mines can be multi-level. Studies in [113] reveals that mines can go as deep as 1165m. A typical coal mine although is 387 feet only. An underground coal mine on the other side can drive up to 2,500 feet deep in the Earth [83]. Uranium mines are the most extreme cases, they are three times deeper than underground coal mines. IoT in surface mine scenario is like IoT in underground agriculture (IOUT). Hence, author's description of IOUT architecture from [134] is referenced here. There are certain functionalities desirable to understand before discussing the architecture. Research in [86] helps to explain few similar and recognize other requirements. These can be mapped in context of mines as follows:

Remote management: to maintain the remote control of the mine's internal functioning system, machinery, communication, it's imperative to establish a remote management system. Such a system would ensure robustness of the mine system under rough conditions [86]. Remote sensing keeps track of mine assets which is communicated through channels to the mine engineers.

In-situ sensing: a mine's interior has tough working conditions. Hence, the system requires sustainable sensors which can measure poles and floors, ceilings and walls, mineral exploration, temperature, fire dynamics, mobile sensors, thermal detection are some of the parameters that requires real-time sensing.

Wireless communication: as per the literature, over the air (OTA) communication is the most reliable type of communication mechanism against the multi-depth rock nature of mines and challenging interference environment. Other forms of communication can still be applied but they have proved slightly ineffective which gives OTA priority over the them.

Interconnection of field machinery sensors, radios and cloud: for achieving real-time analysis of sensor data and communicating decisions it's imperative to have faster, fool-proof device interaction.

Real-time decision making; drilling information, footprint of the internal activities, logging, presence of sensitive biological components should be communicated to managing engineers and authority in real-time

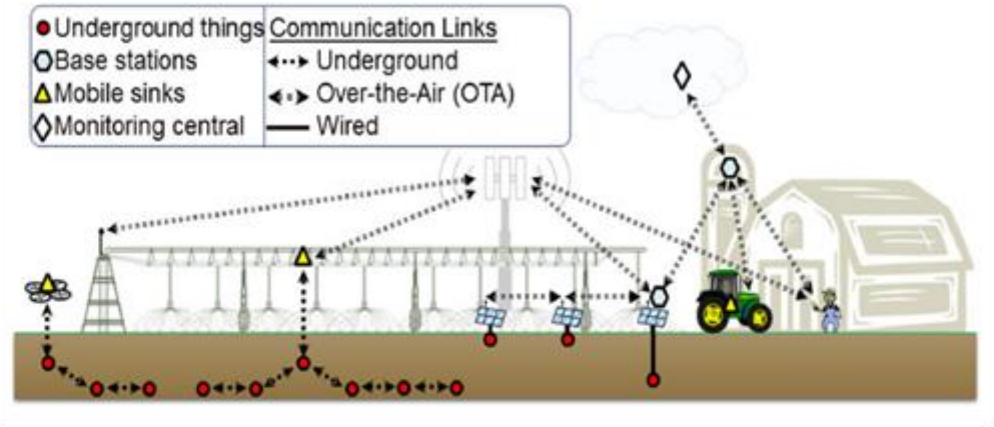


Figure 9. Surface Mine Network Architecture [17]

These requirements give rise to indispensable components such as underground things (UT), base stations, mobile sinks and cloud services as shown in Figure 14. An underground mine, on the other hand, can be single depth (surface mine) or multi-depth (tunnel mines). Tunnel mines introduces new types of challenges. These challenges can primarily affect communication. For example, types of tunnels, physical structure of mine, whether it's a coal mine or metal mine, line of sight. Authors draws a diagram of a typical underground mine from research done in [145]. Authors in this paper suggests that a tunnel mine should consists of wireless communication technologies and devices, sensors and nodes. These nodes are of three types: mobile node, fixed node and sink nodes.

- Wireless communication technologies: These technologies are required for reliable and robust communication such as Radio Frequency Identification (RFID), Wireless Fidelity (WiFi), Bluetooth, World Interoperability for Microwave Access (WiMAX). For research done in [128], present an analytical channel model, a multimodel which emphasizes upon the dire need of reliable and efficient communication in underground network. If needed, the model presented in [145] can incorporate this multimodel for establishing robust communication.
- Sensors: these are for collecting security parameters and transmitting information for underground monitoring.
- Mobile Node: it's an unstable node carried by mine workers for personal identification. These contain tags and related tag-data to be transmitted to receiving node (wireless or wired).
- Fixed Node: placed on either side of the tunnel for communicating with mobile node and to trace identity of miner.
- Sink Node: placed at wire network port, for analyzing and processing the information from the fixed node and then transmitting to the control center.
- CP (Communication Protocol): is the communication protocol between multiple sensor nodes.
- EN (environment): mine environment including shape of the tunnel, concentration of gas, humidity, temperature etc. [145]

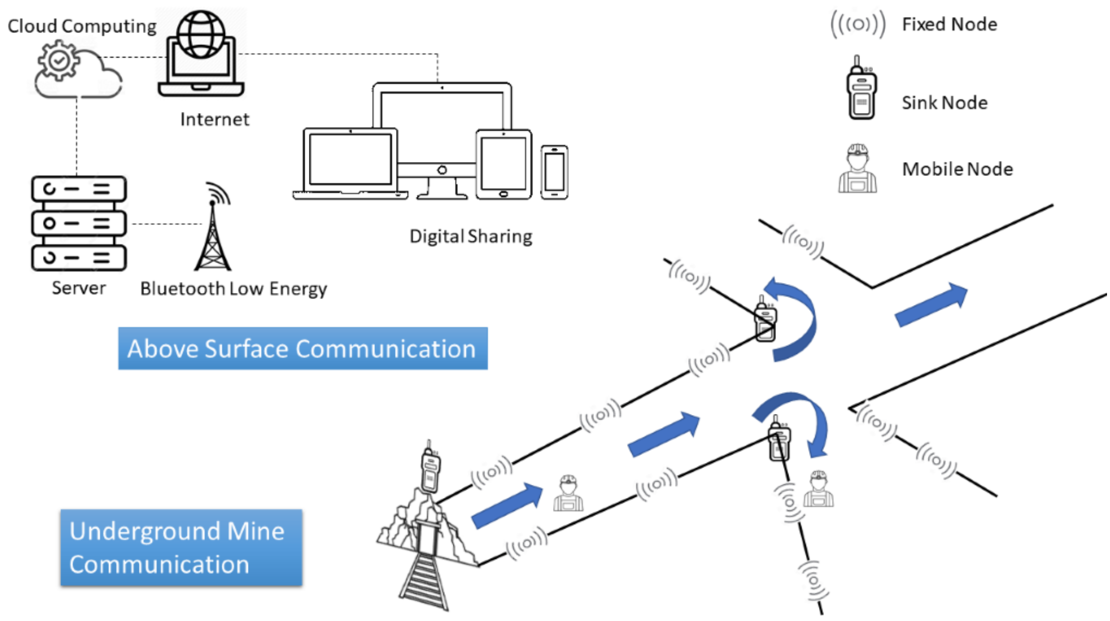


Figure 10. A typical underground mine [16]

IoT in Energy Systems

An IoT architecture is made up of many different parts. Two of the main parts are sensors, which gathers the data to be sent over a network, to actuators, which are what performs the different actions, such as turning an outlet on or off, or changing the temperature on a thermostat [1]. For the data to get to the cloud and get back form the cloud, they must go through a gateway, which connects the IoT device to the internet. Since most of the devices don't have much memory or processing power, it is common to have a cloud gateway that compresses and secures the data for transport between the field gateways, and cloud IoT services. In order to ensure effective transport of input data to the storage location, a streaming data processor is used [1].

Once the data is uploaded to the cloud, it is uploaded to a data lake that stores the data until it is loaded to a big data warehouse [1]. In a big data warehouse, it is preprocessed and filtered so that it only contains cleaned data. Data analytics are then performed from the data in the big data warehouse and gains insights based on the data using correlations and patterns from algorithms created [1]. With data machine learning, new models are created and then tested by data analysts and are used if they work [1]. Once all the data is processed, it is sent to the actuators for commands; such as if rain is detected smart windows can close if they are open, or if the temperature is supposed to be cold, the thermostat can be adjusted [1]. Users are also able to see what is going on with user applications because they allow the user to manually control devices and monitor what their devices are doing. All these devices are tied together for a whole IoT architecture [1].

An example of an IoT Architecture is intelligent lighting where data is taken from the environment, whether it be light, sound, or movement [1]. The actuators in the example are the light switches that turn the light on and off. All the data from the sensors are stored in the data lake [1]. The big data warehouse has data, such as habits, that are based on the day of the week and the energy cost of the area [1]. The user then has a mobile app, the user application, where a map of the home is located, and a user can see what lights are on and off [1]. The lights also use data analytics based on schedules whether they are learned, or they are manually entered by the user, and then changes the lights to be as energy efficient as they can be [1].

Sensors also monitor the outside's natural light and send that data to the cloud and when there is not enough daylight, the lights are then turned on [1]. Machine learning is used by the devices to also turn lights on and off [1]. An example is if the sensor knows the user leaves at 8 AM and come back at 7 PM, then the lights can turn on 5 min before the user comes home so they are on when they get home [1]. This type of architecture can also control other smart home devices.

IoE is starting to become prevalent for the smart grid. The technologies used are devices with microcontrollers and microprocessors that can share information [123]. Devices in IoE must not only be reliable but also be protected against cyber-attacks or unintentional disturbances [123]. The management of generation level resources used to be carried out by using local commands. The system operator was able to control much from a remote control but had to send commands or instructions to a local operator to perform [123]. Grid management is becoming more sophisticated than ever because of the amount of renewable energy resources, the increased number of electrical vehicles in the near future, and the demand of an ever-increasingly high load [123]. In addition to all these new additions to the grid the need for demand-side, medium-scale, or small-scale distribution generation (DG) will be higher [123]. With all the changes in the grid the need for automation and IoT is much needed.

Currently, the operator must deal with a high level of uncertainty and volatility along with restraints that the grid currently has [123]. To improve these issues and to retain security, stability, reliability and environmental sustainability of the power system, IoT devices can solve these problems. In IoT-aided grids, demand and supply can be automatically and accurately monitored and will be able to supervise more of the grid remotely [123]. IoT technologies being used integration with different traditional and renewable energy recourses helps ensure the dynamic and static security of the power system [123].

The smart grid 2.0 is the next generation of smart grids that are looking to implemented around 2020. In the 2.0 model, there will be interactions between supply-side and demand-side and it will utilize the smart meters, share of energy, and sharing of information between key players over network infrastructure [123]. The model will be plug and play meaning where when the gird demands more power, it is as easy as plugging into an outlet to do so. In this new model, it will help utilities being able to monitor anywhere in the grid from the grid operator and can be changed remotely [123]. This helps improve the electricity market greatly by increasing the trading in power exchanges on an internet-based platform for peer to peer trading [123]. The adaption of the new smart grid will be easy due to the focus on smart metering in the last smart grid infrastructure. With the increased real-time monitoring, visibility, and automation for the grid, it will increase the response time to bring the grid back online after an unforeseen outage by making automated changes [123].

In order to make the grid a smart grid, all of the critical points of the distribution network must have IoT infrastructure in place. Figure 1 below shows the IoT Architecture in the distribution level. The first part of this process has already been done for a lot of utilities, which was the installation of smart meters [123]. IoT is the active distribution network which is the energy resources such as diesel generators, gas units, wind and solar units, micro-turbine units, and energy storage units [123]. IoT is being used in these to change the generation schedule to match what the demand of the grid is at the time [123]. IoT is starting to become more popular also in the microgrids of the transmission system. Currently, the microgrid is separate from the main grid and there is a separate operator on the microgrid [123]. With the implementation of IoT in the microgrid, it will give the main grid operator better insight and control into the microgrid, which can help account for the generation of energy for the microgrid [123]. With this added benefit the main grid, an operator can account for power generation in the microgrid which can make a company more profitable [123].

IoT in energy systems is starting to become more common in the smart city architecture with different types of IoT sensors and telecommunications infrastructure. IoT is designed where devices such as solar-powered streetlights can be monitored to see if there is adequate energy being provided to them. Otherwise, they can get power from the main grid supplied to them [123]. The power grid now must account for all new electronic vehicles needing more electric consumption. In the parking garages, IoT devices are being used to sync with the electric vehicles to try and calculate the power need from the grid. With so many of the new devices becoming powered by the electric grid, there are a lot of IoT devices in buildings to keep the building running more efficiency [123]. Devices on the grid are required to have IoT for network connectivity, which can either be connected to an access point, LTE, or 5G protocols coming soon [123].

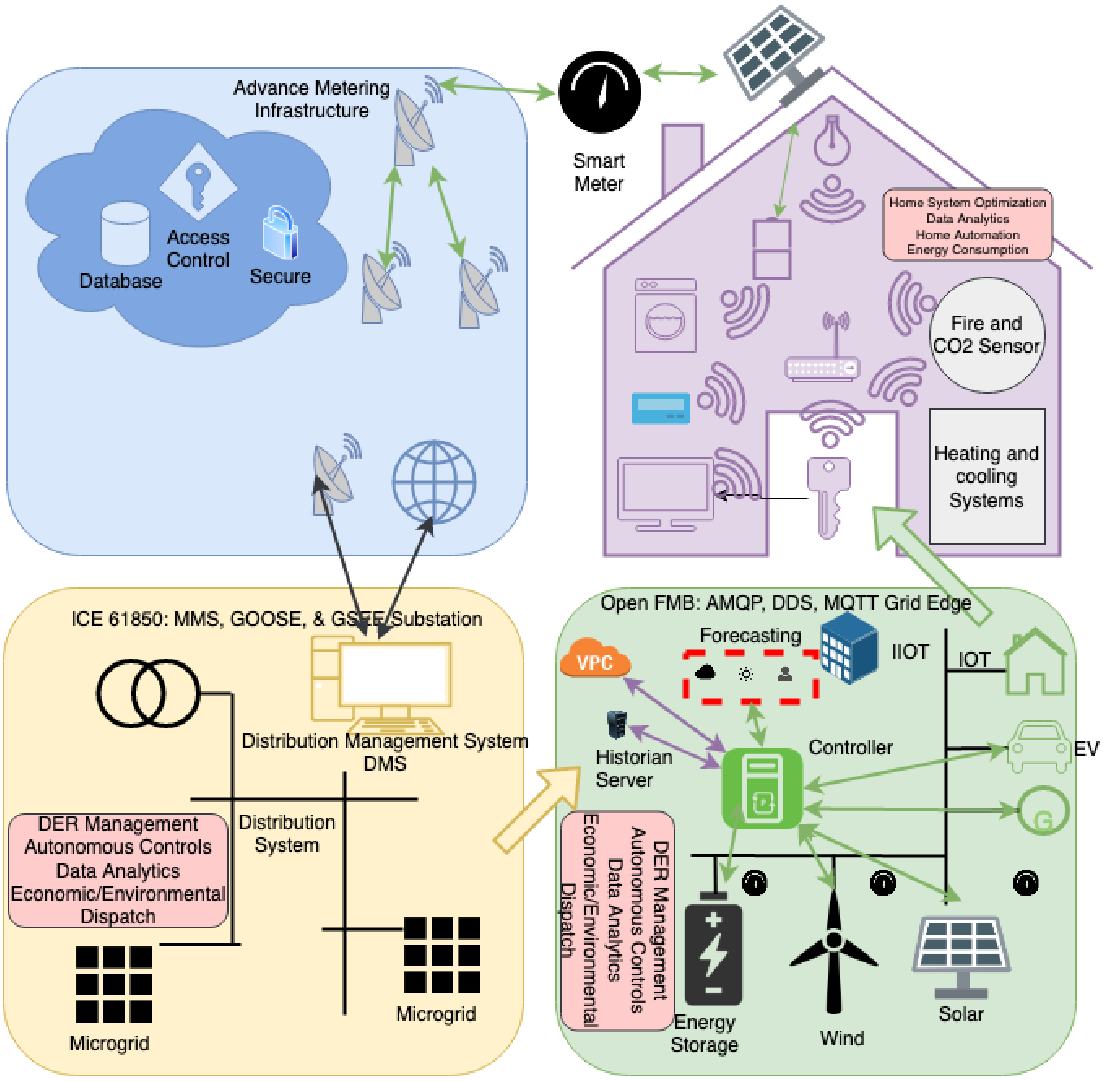


Figure 11. Power Systems

Grid Architecture is designed to help manage the complexity of the grid modernization process. For smart grid adoption to go well, it is required that the architect techniques are adopted early in the modernization process [129]. The US Department of Energy has an Energy's Grid Modernization Initiatives to work on motivating and transforming today's legacy grid. There are five key trends that are driving the transformation: changing mix of generation, need for improved reliability and resilience, opportunity for consumers to participate in the market, replacement of aging infrastructure, and the connection of electricity information and control systems [129]. Part of developing the smart gird is that they must first identify the systemic issues, which they look at what parts affect all parts of the grid, not just single components [129]. Then during the design, they must apply grid architecture methodologies. Part of that is getting rid of the siloed infrastructure and using a layered design that brings all components of the grid together. Finally, they must create grid architecture documents in order to have a full understanding of the grid and to find where failure points might be [129].

A recommended architecture called the EnergyIoT Conceptual Model into 3 domains, Energy Systems Cloud, Energy Services Cloud (DevOps), and Operations Technology (OT) as shown below

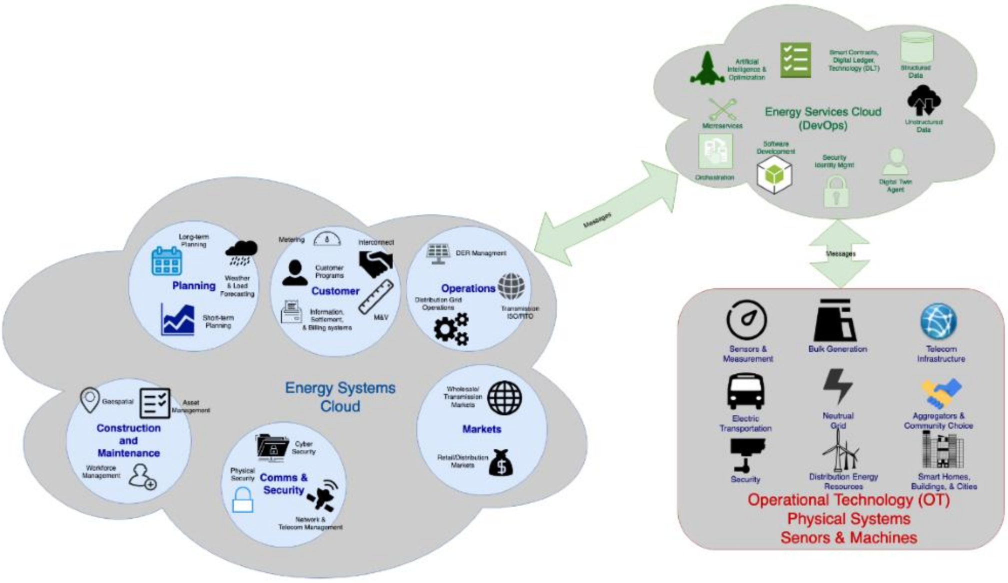


Figure 12. IoT Domains [95]

in Figure 2 [95]. Two of these domains are considered the IT grids which are the Energy Systems Cloud and Energy Services Cloud. The benefit to these two grids is that they can be hosted anywhere whether that be an on-premises data center or in the cloud [95].

The OT Domain makes up the physical assets that are part of the power grid [95]. In this domain, a neutral grid is ideal where the assets communicate and cooperate with one another to keep the grid stable and resilient [95]. The subdomains that are included in the Operational Technology domain are sensors and measurement, bulk generation, telecom infrastructure, aggregators and community choice, smart homes, buildings and cities, distributed energy resources security, electric transport and neural grid [95].

The Energy Systems Cloud Domain is the utility perspective of application systems, devices, knowledge, and processes that are required to maintain and keep the grid running efficiently [95]. This cloud helps utility companies plan for the short- and long-term future to forecast power usage [95]. With the data discovered, this cloud decides what construction and maintenance is needed in the grid and helps locate when problems are physically located in the gird [95]. In order to make the gird safe and manageable remotely, communications and security are in this cloud to help ensure physical and cybersecurity for the grid [95]. Customers benefit from the Energy Systems Cloud domain as it helps with better analytics on their bill to show different ways to lower their energy usage [95]. The cloud also helps with what is needed from the market as it can help utilities decide if they have excess energy to sell on the market or need to buy more energy to keep the grid running [95].

The final cloud is the Energy Services Cloud (DevOps) which is considered the heart of the architecture that ties two of the clouds together [95]. It includes services such as smart contracts, structured data, unstructured data, digital twin agent, security and identity management, source code management, orchestration, and microservices [95]. This layer helps with interoperability and streamlines the communication between sensors and the grid. This helps support the rapid development in the energy IoT market by making it simplified to grab the data analytics in the same format as the development of tools [95]. The Energy Services Cloud is designed for data and data supporting services in this data-centric architecture [95].

In general, smart city IOT consists of numerous layers within their architecture. The abstracted layers are as follows: sensing and data collection technologies, transmission technologies allowing for data aggregation, a data processing layer where raw data is processed and analyzed, and the fourth layer in the form of an application layer that displays the information generated in a meaningful way to the end user of the system [60]. The way the 4th layer displays data will be

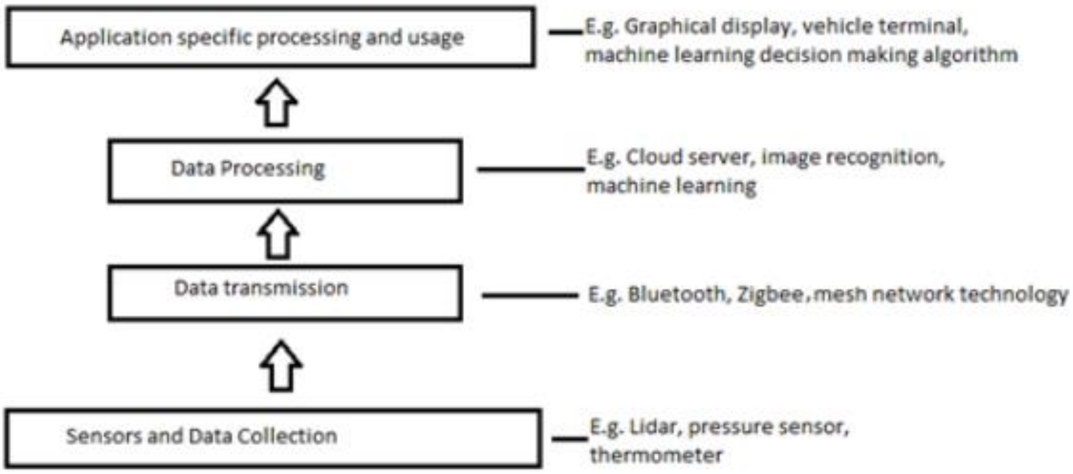

Application specific processing and usage
E.g. Graphical display, vehicle terminal, machine learning decision making algorithm
Data Processing
E.g. Cloud server, image recognition, machine learning
Data transmission
E.g. Bluetooth, Zigbee, mesh network technology
Sensors and Data Collection
E.g. Lidar, pressure sensor, thermometer

Figure 13. General architecture in smart city IOT[60]

dependent on the specific use case and service that the system performs [60]. A zeroth layer could also be counted that consists of the bare minimum equipment that would have existed before being adapted into smart devices capable of intercommunication. In the waste management application of IOT, it would consist of basic plastic garbage bins without any sensor or identification system, stock garbage trucks without any advanced routing systems or sensors etc. With this general abstracted architecture in mind, we can look at how specific implementations of IOT systems in smart cities are done to compare them.

Food supply chain management

Within the US, food imports have increased by 22% between the years 1997 and 2005. Due to the large increase in food imports and the challenges of keeping track of all imports in a manner which would prevent food spoilage, contamination, and wastage among other things, a smarter, technologically based system of tracking food has the potential to make great improvements to the current system [150].

The first physical layer is comprised of sensors installed at each node of the food supply chain: farm, transportation, warehousing, transportation, and market [150]. Above this layer is second layer responsible for aggregating the data collected by these various sensors which is referred to as a data bus. The third layer is comprised of a data storage system and server processing system working in tandem to convert the aggregated information into usable information. Finally, this useful information is passed on to a display and visualization system [150]. Overall, the architecture of the system closely follows the general architecture for all IOT systems. However, there are unique concerns within the food supply chain management system that need to be mentioned.

Due to the volume of food being imported it is unfeasible to gather data from every food import system within a city, much less analyze all of it. As such, the researchers proposed using only tracking a small sample of the food being imported using this system [150]. The small sample of food that they collect data on will then be used to extrapolate possible food contaminations using various data manipulation techniques [150]. The sheer volume of food means that having to check and scan each item would be too costly for food wholesalers to implement [150]. In addition, the data collected by sensors must be processed as close to real-time as possible [150]. This is to ensure that if spoiled food is detected, it can be dealt with in a timely manner before it has been prepared or consumed. Early detection and warning of spoiled or contaminated food also would allow health officials to quickly investigate the source of the food in an attempt to find where in the food supply chain the contamination occurred so that they can catch other shipments of contaminated food that were not previously known about. The solution to this issue is to use algorithms and modelling to be able to make reliable conclusions from only a small sample of the greater whole [150]. It cannot be solved with a modification to the architecture of the system, but only by scaling down the system to maintain reasonable deployment costs and using data manipulation to make up for the significant loss of data volume that would have been collected.

Smart meters for electric grids

Smart meters are a useful piece of technology that tackles certain challenges conventional power meters had. They can gather information on power quality, reliability, and energy usage [14]. The implementation of smart meters would not only benefit utilities companies but the end consumers as well. Consumer usage of electricity can be reported back to the company for analysis. The company can then use collected data to determine if services are at an adequate level [14]. For example, poor maintenance of power transmission lines could appear as irregular currents at the consumers home which would be reported by the smart meter back to the company who are now aware of the situation and can perform maintenance. Data analytics on consumer usage can be sent back to the consumers to help them plan their usage and allow them to monitor their own power consumption [14].

The architecture of these smart meter systems proposed by Al-Turjman and Abujubbeh[14] are as follows: first the data collection layer in the form of the actual smart meter devices installed at each consumers home. The second layer consists of the networks which are used to aggregate the data that are deployed on a neighborhood scope called Neighborhood Area Networks (NAN). Within this same layer is a Wide Area Network with a larger scope of the internet. The WAN is supposed to carry data from the relatively small and local NAN to the end point, the utility company, where the data will be stored, processed, and then analyzed. The utility company servers therefore comprise the third layer while any data sent back and displayed on consumers web portal for example would be considered the 4th layer. Because of the potential for data to be processed at the utility company but then sent back to the consumer, the architecture is more complex as data may need to travel from a higher layer, layer 4, back down to layer 3 to be transmitted back to the homeowner for consumption.

Smart Speed Control

Adaptive speed control systems were proposed in order to help prevent accidents during inclement weather. There were 1.2 million deaths worldwide due to traffic accidents globally in 2016 [14]. This indicates that despite driver training, numerous safety messages put out by all countries, people are still in danger. Adaptive speed limits are one system proposed to help prevent these accidents from occurring.

In this system proposed by Al-Turjman [14], layer 1 of the architecture is composed of not only sensors used by vehicles to detect road condition, but also road side units, called Local Controllers, capable of monitoring volume of traffic, the smartphones of drivers, and even uses the reports made by patrol police and weather forecasting stations. Vehicles also have specific equipment mentioned as Speed Limit Transmitters and Receivers (SLT and SLR) which receive changing speed limits wirelessly, and in-vehicle micro controller that monitors the vehicles speed and checks it against the broadcast current speed limits as well as Mobile Controllers used to detect road conditions. If the driver is found to be in violation of the speed limit, this microcontroller may either issue a warning or report the driver back to the management system where it can be forwarded to law enforcement if needed.

Layer 2, the data communication layer, relies on a combination of networking and wireless technologies to transmit information to and from the vehicles. These technologies include 4 or 5G modems installed in vehicles and roadside stations to communicate back speed and road conditions to the higher layer, Management and Control Center (MCC), which is responsible for managing the road and setting speed limits based on other aggregated data. Public switched telephone networks are also used by the MCC to communicate with the SLT and SLR's.

Finally, there are the MCC's and Driver Records Server (DRS). These devices are responsible as the point where data is aggregated from not only drivers and vehicles on the road, but from other pertinent sources as well such as patrol cars and weather station forecasts. They are also responsible for the data processing as well, meaning these 2 systems are essentially layers 3 and 4 combined as they not only handle the decision making, but also make the reports and generate useful information to be consumed. The decisions they make are relayed back to the vehicles through the same data channels used to initially transmit data from the vehicles to the servers. In addition, the cellular network can be utilized by the MCC to issue warnings or tickets to drivers via their cellphones. The DRS acts as a separate storage and processing center that works in tandem with the MCC. While the MCC is responsible for traffic and the actual monitoring and data processing of roadside conditions via vehicle, patrol, weather, and roadside unit data, the DRS is used to help enforce these adaptive speed limits by maintaining a list of drivers so violators can be ticketed. Because of the potential for speed limits to change rapidly, it may be difficult for law enforcement to adapt quick enough to catch people in violation of the speed limit. As this adaptive speed limit system is already relying on data transmitted from vehicles, it makes sense to also equip vehicles with a method to self-report the driver if they are found to be in violation.

Waste Management

In the waste management application of IOT within smart cities, one possible architecture the architecture of the proposed systems can be divided into 3 layers. The first layer is the physical layer which contains the low-level items that enable data collection and sensing information to be collected. This would include devices such as weight sensors on garbage trucks and garbage bins to sense how full they may be. This layer also includes RFID tags to allow the system to identify different objects as distinct from each other [16], for example to tell the difference between a garbage dump on street A rather than street B which allows the system then to plot optimized and time or fuel-efficient garbage collection routes to take [16]. Sensors can also be incorporated at this level to detect full or empty garbage bins that need to be collected or incorporated in the garbage trucks themselves to monitor their remaining capacity compared to the remaining volume of garbage yet to be collected on its route.

The second data communication layer for this proposed system would be the low-power radio communication processed using an ad-hoc network [16]. This system would be implemented with the use of IPv6 over a low power network. In addition, a smartphone network of drivers can be used as the backbone of an ad hoc network allowing the sensors and devices at the lower layer to transmit information.

The third layer of this proposed system is the infrastructure that would support the high-level decision making and route optimization called dynamic scheduling and routing. The system that would be responsible for these calculations and actual processing of raw collected data is called Decision Support System [16]. This third layer would contain the physical hardware needed to process the data aggregated using the wireless technologies and transmission systems in layer 2 to make some useful information out of them. A potential layer 4 candidate for this system not explicitly mentioned in the original proposal could be the use of web connected smartphone application that receives new routing instructions from the dynamic routing generated from the DSS, or alternatively a basic terminal located in garbage trucks that would receive the updated routing information from the DSS and display it visually for the waste management employees to use.

Similarities

In general, all the examined smart city systems follow the general architecture proposed in [60]. The architecture makes a lot of intuitive sense, a base layer responsible for data aggregation, followed by successive layers that allow for intercommunication, followed by data processing, then data presentation. While the various technologies and implemented protocols differ, the basic architecture of all information communication technologies remain the same in IOT across almost all implementations.

Differences

Looking at the various IOT systems proposed, the key differences lie within the specific details of each system. Certain systems have many more sensors than others based on their specific use case and cost factors. Certain applications require more data collection in order to make decisions.

doi:10.20944/preprints201912.0276.v1

Adaptive Speed Limits and Food Supply Chain monitoring will require many more sensors and devices distributed in many places for the system to be effective. Adaptive Speed Limits not only requires multiple devices to be installed on each vehicle in the city, and they must be installed across all vehicles within the city as failure to do so means certain drivers will not be privy at all to changing speed limits. This would make the entire system moot as those drivers would put drivers who have integration with the system in danger by not following the current speed limits. Food Supply Chain, although they have acknowledged that the scale of food imports within a city to be too great to fully monitor, will still need to have devices located at various ingress points or warehouses within the city to monitor the condition of foods being imported. Compared to systems like the smart meters which only require a single device to be installed at the consumers' homes, and the basic networking equipment and infrastructure needed to pull information from the smart meters back to the utility company, smart meters seem much simpler to implement. This difference in terms of number of sensors required for each IOT system, as well as supporting infrastructure is perhaps the most important difference between smart city IOT. While all these projects are good and can undoubtedly improve the lifestyles of the city's denizens, they are not all equal in terms of deployment costs, maintenance, and other factors.

Some of these systems like adaptive speed limits will also require standardization of manufacturing as they require all vehicles to come pre-equipped with installed components that will be leveraged for the system. Either consumers will be forced to purchase these devices and install them on their own through legislation, or all vehicle manufacturers will need to install necessary components themselves and standardize that practice across the industry.

3. Wireless Communication Technologies

The backbone for IoT systems is the wireless communication which should be able to transport data from sensors to a database through secure, reliable, low power, and low-cost networks supported by a variety of protocols and standards. The key parameters that these wireless technologies should address are range, data speed, power consumption, security level, cost, reliability, etc. The communication techniques used in IoT are mainly categorized into two main variants 1. Short-range Communication and 2. Long-range Communication [21]. Short range communications have signals that can travel only a few meters and are used for topologies such as Personal Area Networks (PAN) and Wireless Body Area Networks (WBAN) while long range communications as listed below in the table are used for transmitting data from the base station to central nodes located several kms away. The remainder of this section will cover the paradigms of wireless IoT technology research and provides pros and cons for them.

3.1 NB-IoT

Narrow Band-Internet of Things (NB-IoT) is a recently introduced wireless technology standard to address Low Power Wide Area (LPWA) needs of IoT devices. It is classified as a 5G technology and has been incorporated by Third Generation Partnership Project (3GPP) Release 13 in 2016 [91]. NB-IoT communications provide long battery life, low device cost and signal coverage extension in delay-tolerant low data transmitting applications. It also has the system capacity to connect large fleets of devices efficiently with good spectrum efficiencies.

NB-IoT can achieve communication range up to 15km and at the same time maintain relatively high speeds. It can also support a minimum of 52,547 nodes per base station. Communication channels are Bi-directional with high uplink and downlink data transfer rates. As it has adopted Half-duplex for higher efficiency the operating frequencies of uplink and downlink are different and hence only allows either transmitting or receiving at a time. Another interesting feature of this technology is that it can coexist with current wireless technologies such as LTE and 2G/3G/4G, and therefore be easily deployed. This new technology is finding more and more takers from healthcare IoT solution providers because of its secure, long range, high energy efficiency connectivity, and multiple device support.

NB-IoT adopts state of the art 3GPP S3 security implemented at both transport and application layers. The security mechanisms available in this technology are: i) Device/Network mutual authentication, ii) Securing of communication channels, iii) Ability to support "end-to-end security" at the application level, and iv) Secure provisioning and storage of device identity and credentials [65]. Encryption mechanisms are also implemented to counter any eavesdropping threats and to protect sensitive health care data. NB-IoT with all the security options in place can provide secure network for deploying healthcare applications.

3.2 Wave

To overcome the shortage of WLAN's applications in a highly mobile environment, several research works have been carried out to study another communication technology, WAVE, which is defined in 802.11p [137]. WAVE communication technique is de- signed specifically for inter-vehicular communication. The technique can be used in V2V and V&I models for data exchange between moving vehicles and between vehicles and the roadside infrastructures. IEEE 802.11p LAN system uses 5.15-5.25, 5.25-5.35 GHz and 5.725-5.825 GHz unlicensed band. Consequently, the supported data rate is 6, 12 and 24 Mbps. The system contains 52 subcarriers which can be modulated using BPSK, QPSK, 16- QAM, 64-QAM. IEEE 802.11p contains the PHY and MAC layer protocols. The PHY layer adopts OFDM transmission technique and OFDM subcarriers have frequency spacing at 156.25 kHz, demonstrating a bandwidth of 10MHz. The data packet is encoded using one of the modulation techniques mentioned above. At the MAC layer, CSMA/CA is adopted to reduce the prob- ability of data collisions. To further avoid overloading effects in CSMA/CS mechanism, adding other algorithms (e.g. SAE J2945/1 and ETSI via DCC) becomes necessary [25].

3.3 WiMAX

WiMAX, named Worldwide Interoperability for Microwave Access, belongs to a family of wireless broadband communication standards, regulated un- der IEEE 802.16. In IEEE 802.16 defines both PHY and MAC layers. The WiMAX was formed in 2001 to promote this technology as an alternative to DSL and cable-based communication techniques. IEEE 802.16m was considered as one of the candidates for 4G network, competing with the LTE Advanced standard. The physical layer of WiMAX features easily configurable data rate with available selected channel bandwidth. The WiMAX is considered to provide portable mobile connectivity to city-based applications, such as IoV system and wireless alternative to DSL. This technology can potentially provide data, telecommunication and IPTV services at the same time. The PHY layer operates in a frequency range of 10 to 66 GHz. The data transmission utilizes scalable OFDM in which MIMO protocols are employed. The most advanced WiMAX version, 802.16e, increases the signal coverage, reduces the power consumption, and boost up the bandwidth efficiency. The WiMAX MAC layer adopts a scheduling algorithm so that the subscriber station is only required to complete one network entry. After permission from the network entry, the subscriber station will be allocated one unique access slot which cannot be used by other subscribers. The scheduling algorithm brings benefits in bandwidth efficiency, prevents net- work overload and over-subscription, and controls Quality of Service (QoS) parameters easily with proper time-slot assignments.

3.4 4G/LTE

4G/LTE potentially provides vehicles non-stop network connectivity. With recent progress in the 4G LTE network, the transmission speed is gradually stable at 100 Mbps for downlink and 50 Mbps for uplink, which demonstrates a significant speed boost comparing to 3G networks. The 4G LTE is considered as one of the irreplaceable candidates in IoV wireless communication system due to its high speed, low latency, and other services. However, 4G LTE also gradually reveals its drawbacks in power savings. The state- of-the-art system employs OFDM technology, specifically called SC-FDMA, for data uploading. Consequently, power efficiency got primarily improved. Discontinuous reception (DRX) technique lowers down the downlink power consumption. DRX reception algorithm periodically wakes up devices for messages and put devices in speed for the remaining time. At the same time, improving power consumption and channel delay brings up tradeoff in which applications plays an essential role in making the final design decisions.

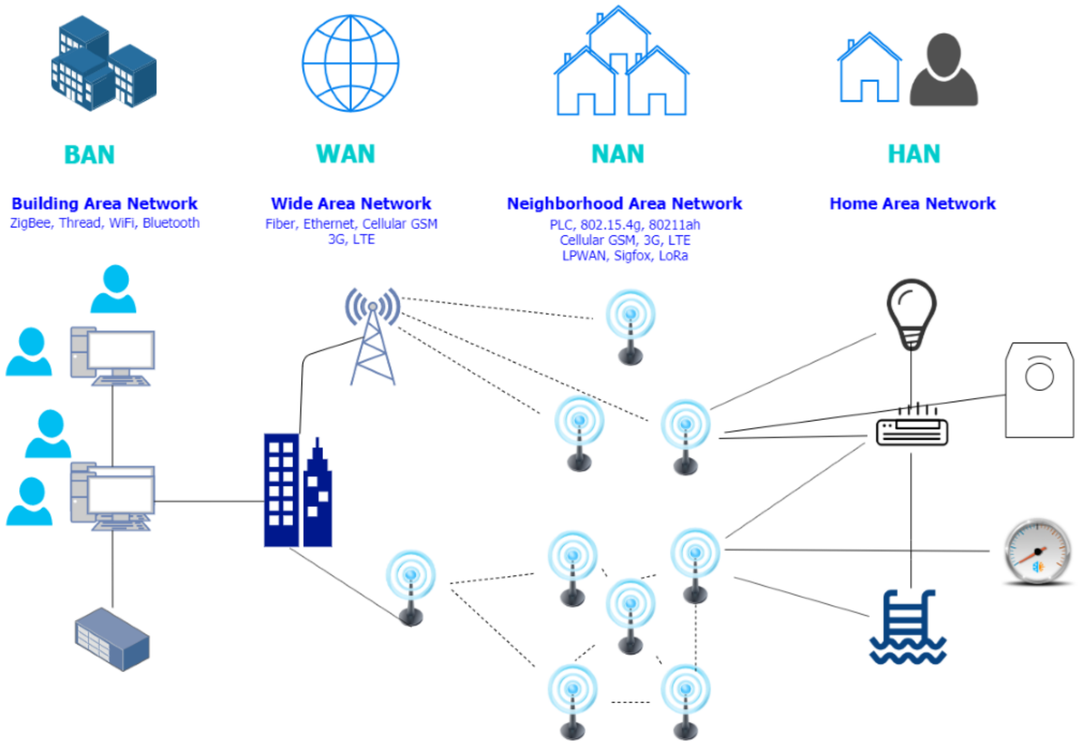


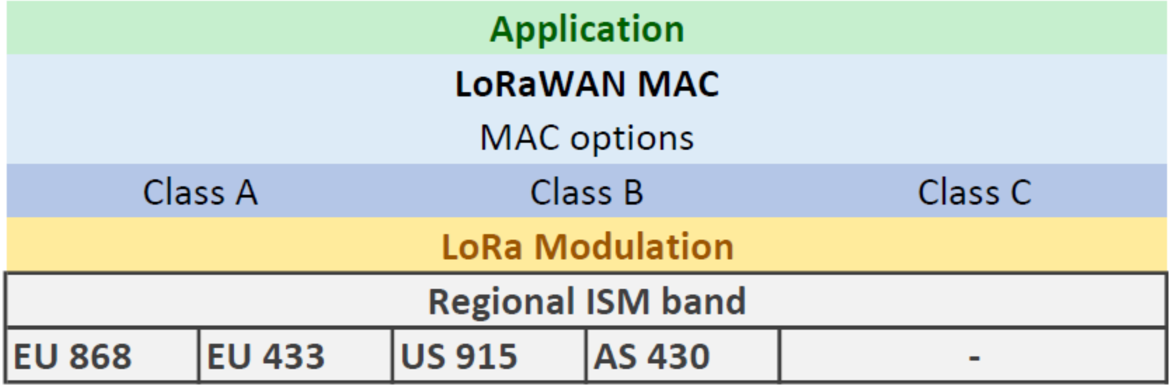
Figure 14. Wireless Networks

3.5 Thread

Thread is an IPv6 based, low-power mesh networking protocol [18]. Thread was developed to be secure, future proof and available at no cost [18]. It does require an agreement and expects the user to adhere to a EULA which subjects members to an annual membership fee unless used for academic purposes [18]. Thread uses a protocol called 6LoWPAN which runs on the IEEE 802.15.4 wireless protocol with mesh communication just like ZigBee and other wireless communication protocols [18]. Thread is also IP-addressable and has cloud access with AES encryption [18]. This makes thread useful for LAN implementation as the IP addresses can be utilities to connect multiple IoT devices to the same network. Great uses for this are smart devices on home networks and research-based networks. 6LoWPAN works based on the use of an edge router or as thread calls them "Border Routers" [18]. These routers, unlike other edge network routers do not use any application layer states because the forwarded datagrams on done on the network layer [18]. This greatly reduces the processing power burden on edge routers because 6LoWPAN is not aware of application protocols and changes [18]. Thread, being a protocol designed for IoT devices, addresses a few of the IoT design requirements through its low processer use and security encryption.

3.6 SigFox

SigFox is a global network operator founded in 2009 and based on France [6]. They build wireless networks to connect low-power objects like smart meters [6]. SigFox uses a differential binary phase-shift-keying and Gaussian frequency-shift keying method that enabled them to communicate using the Industrial, Scientific and Medical ISM radio band [6]. This band operates at 902MHz in the US and because it operates at such a low frequency, it allows the signal to pass freely through solid objects called "Ultra Narrowband" and like other IoT protocols, requires very little energy to propagate [6]. The network topology is based on a star topology and requires a mobile operator present to carry the traffic throughout the network [6]. In October of 2018, SigFox had covered 4.2 million square kilometers in about 50 countries with a goal of 60 by 2018 [6]. SigFox provides a great example of what integrating IoT technology with low frequencies can provide from a networking standpoint. They have also partnered up with LPWAN industry giants and attempted support for bidirectional communication [6]. The current standard for this protocol allows support for 140 uplink messages a day with a payload of 12 octets and a data rate of up to 100 bytes per second [6].


Application

LoRaWAN MAC

MAC options

Class A	Class B	Class C

LoRa Modulation

Regional ISM band

EU 868	EU 433	US 915	AS 430	-

Figure 15. LoRa Layers

3.7 802.11 Standards and Wi-Fi Alliance

Often smart cities have an infrastructure that relies on short distance communications with a larger bandwidth due to homes and offices having centralized devices that are connected to wireless devices throughout the house or building. One of the most used ways to communicate not only in smart cities but in general wireless LAN networks is using 802.11 wireless standards. IEEE in the early 1990s assembled a team of people to develop a wireless standard which would later become 802.11. Due to the start of 802.11a and 802.11b standards, the new era of communication began.

The 5 GHz band was not as dense because many countries opened those unlicensed frequencies for use. 5 GHz channels are numbered from 36 to 165, which can vary depending on the country that the network is residing. Starting channel 36 has a frequency of 5180 MHz and the last channel, 165 has a frequency of 5825 MHz Now though this an outdated technology, is still in use in some areas which is why it is worth mentioning. With data rates of 54 Mbps reaching distance anywhere from 25 ft to 75 ft indoors [77], 802.11a speeds are not excessive compared with what is available today. The 802.11a standard was not very popular and was overshadowed by the 802.11b standard, nevertheless the 802.11a standard provided a foundation on which future standards could be built up on and improve. A downfall the 802.11a standard's higher frequency was that the distance can be reduced significantly if an obstacle such as a wall or a door was placed in the line of communication between two devices.

During the same year of 1999, IEEE adopted the 802.11b standard that has heavily used up to this date. The 802.11b standard uses 2.4 GHz spectrum. The lowest frequency starts at 2401 MHz on channel 1, with an additional 14 channels in which there is a range of2.4 GHz with each channel span being 22MHz. Utilizing 2.4 GHz spectrum gave an advantage to the 802.11b standard over the 802.11a standard in reaching further distance but it had to compromise on speed. The 802.11b standard has a data rate of 11 Mbps up to 150 ft indoors [77]. Just like the 802.11a standard the distance of communication between two devices can be shortened by physical obstacles that are in the way. Additionally, a being lower frequency than the 802.11a standard imposes a problem of sharing the frequency with microwave ovens, garage door openers, cordless phones, baby monitors, etc. [77] which brings more interference to the communication.

Although the 802.11b standard was reaching longer distances than 802.11a standard, there was a need for higher throughput, so in June of 2003 a new standard was introduced. It was named the 802.11g standard and most importantly it was backward compatible with the 802.11b standard (IEEE Standard for Information technology 2007). This meant that users can have both standards at the same time during the transition process from one standard to another. Moreover, the 802.11g standard has data rates of 54 Mbps and can reach the distance up to 150 ft just like the 802.11b standard.

In 2009, boundaries were pushed with the development of higher bandwidth in the 802.11 protocol. Due to a desire to reach higher data rates, multiple-input multiple-output (MIMO) and new the 802.11n standard were introduced. MIMO is a wireless system where multiple antennas can be used to transmit data in parallel streams to increase the capacity. Not only do they have higher data rates but the 802.11n standard supports both 2.4 GHz and 5 GHz spectrum. In 5 GHz spectrum data rates are up to 600 Mbps. This is not the case for 2.4 GHz spectrum where maximum data rates are 104 Mbps (IEEE Standard for Information technology 2007). Another capability of the 802.11n standard is that it can use both 20 MHz and 40 MHz channel widths on distances up to 175 ft indoors. This distance is calculated on 2.4 GHz spectrum where it would be reasonable to conclude by previous examples that maximum distance on 5 GHz spectrum will be shorter.

Once again, at the beginning of 2014 a new standard was announced, and it was named the 802.11ac standard. This time two more channels with larger widths were added, 80 MHz and 160 MHz channels which allow higher speed communication. Unfortunately, the 802.11ac standard only supports 5 GHz spectrum. Being driven by greater speeds than its predecessor the 802.11n standard, the 802.11ac standard uses a somewhat different approach to streaming. The 802.11n standard used four spatial streams where the 802.11ac standard uses eight. Using beamforming technology, the 802.11ac standard allows transmission of data in a specific direction. With larger channels and new technologies, the data rate for the 802.11ac standard is rated at 433 Mbps up to 1 Gbps.

Another standard worth mentioning, is the 802.11ax standard that will be introduced in late 2019. This new wireless standard will be up to 30 percent faster and will have around a 75 percent latency improvement over its predecessor the 802.11ac standard with four times as much data delivery according to Rupert Goodwins in the article about Next-generation 802.11ax wi-fi: Dense, fast, delayed [63]. Furthermore, he mentioned in the article that there are different technologies that standout such as how to handle radio frequencies using 2.4 GHz and 5 GHz spectrum and combining 20 MHz wide channels up to 160 MHz wide. Colors were implemented in the 802.11ax standard, which reduces interference between Access Points (AP) that are using the same channel (Goodwins 2018). With the 802.11ax standard using MIMO and the new technologies mentioned before, it will have great potential in the IoT as well as a piece of spectrum just dedicated for that. For the 802.11ax standard to be fully adopted will take some time make appropriate changes to the hardware.

As the 802.11 standards and subsequent naming convention can be overwhelming to someone who is new to these technologies as well as to regular home user, Wi-Fi Alliance introduced a new naming scheme for the 802.11 standards in 2018 that is much simpler to remember. Table 1. presented below shows new and old naming convention in correspondence to each other. This change is the step towards to easier recognition of standards and cohesion between them. As it has been mentioned before WiFi 6 will have a great impact in the IoT system in the future but until then all the previous standards will be part of the implementation throughout many smart cities as well as everywhere else.

Table 5. Wi-Fi Alliance Generation of Connection compared to IEEE naming convention

WiFi Standard	WiFi 1	WiFi 2	WiFi 3	WiFi 4	WiFi 5	WiFi 6
Networks	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax

	Short-range Communication		Long-range Communication		
	Bluetooth Low Energy	ZigBee (XBee Module)	SigFox	LoRaWAN	NB-IoT
Band of Operation	2.4 GHz	2.4 GHz	868 MHz (Eu) 915 MHz (US)	868 MHz (Eu) 915 MHz (US)	Multiple
Network Capacity	2 nodes	65000 nodes	50,000 nodes	40,000 nodes	53,547+ nodes
Range	150 m	30 m	9.5 km	7.2 km	15 km
Data Rate	1 Mbps	250 Kbps	100 bps	0.25 – 5.5 Kbps	250 Kbps
Security features	Secure Pairing Two keys authentication and identity protection 128-AES encryption	Network key shared across network Link key application-layer communications 128-AES encryption	Private Key Signup 140 messages per day limit Encryption and scrambling methods supported	Unique key for each node Data encrypted using unique key	3 GPP S3 security scheme - includes entity authentication device identification, user identity confidentiality and data integrity
Suitability for Healthcare	High	Moderate	Low	Moderate	High

3.8 Bluetooth Technologies

Another wireless technology that is often used in a lot of devices for different applications is Bluetooth. Bluetooth spans a shorter distance compared to Wi-Fi. Bluetooth started as a short link radio communication technology developed in 1994 by Ericsson and became Bluetooth in 1998. The unique name is derived from the 10th century Danish king who united Scandinavian people [39]. Combining their talents Ericsson, IBM, Intel, Nokia and Toshiba formed a team that is called Special Industry Group or more commonly called SIG to help Bluetooth spread in the market. Bluetooth was pushed to the forefront of adopter awareness when SIG offered this intellectual property to adopters for free, SIG's benefit remained to be the public respect gained of their product as 70 adopter members increased to 3000. Later SIG would only fully release the Bluetooth specification version to the public when it was fully vetted and approved, the adopters had full access to the specification before release [39]. IEEE's 802.15 standard is based on Bluetooth, SIG wanted IEEE to adopt their standard and become an official part of 802 standards, in this instance IEEE was able manage revisions on SIG's standard (IEEE Standard for Information technology 2002).

Bluetooth operates on 2.4 GHz Industrial, Scientific, Medical (ISM) band where the range of the frequency is from 2400 MHz to 2483.5 MHz. This range may vary from one country to another depending on their limitations in the range. Furthermore, Bluetooth comes in three power classes. In class one maximum power output at maximum power setting is 100 mW (20 dBm), in class two 2.5 mW (4 dBM) and in class three is 1 mW (0 dBm) (IEEE Standard for Information technology 2002). Bluetooth's low power consumption helps devices to have better power management. Although Bluetooth is known to consume lower power to function some might think that is also a short distance technology, Bluetooth can have successful communication in class one up to 328 ft. Class one is mostly used for industrial purposes where class two is commonly used for electronic gadgets such as cellphones, headphones, wearable devices, Bluetooth speakers, etc. As transmit power drops so will the range of Bluetooth coverage, so in class two distance is up to 33 ft and in class three is less than less than 33 ft [10].

Throughout the years Bluetooth went through a few versions starting in 1999 with version 1.0 all the way up to version 5.1 which was presented in 2019 by Bluetooth SIG [42]. Throughout the versions new technologies were introduced and faster data rates were achieved. Bluetooth started with a maximum data rate of 0.7 Mbps in version 1.0 and jumped to 3 Mbps in version 2.0 then in version 3.0 up to 24 Mbps. Data rates of 24 Mbps on 3.0 version of Bluetooth were achieved by just starting a connection as a Bluetooth and then transmitting data through Wi-Fi. In version 4.0 data rate went back to 3 Mbps where it stayed all the way up to version 5.0. Bluetooth 5.1 is the new technology called AOA which is short for Angle of Arrival where it uses distance and direction to find location of the device [42].

Due to Bluetooth's wide range of applications and cheap implementation costs this makes Bluetooth one of the primary technologies to be used in IoT and smart cities. Due to not utilizing much power Bluetooth can be used in small devices that cannot sustain power for long. Moreover, Bluetooth's capability to be connected in mesh is an ideal situation for smaller spaces that have multiple devices that need to communicate to each other such as in Small Office Home Office (SOHO) environments.

3.9 *IEEE 802.15.4 standard and Zigbee Technology*

Zigbee is a technology standard created for control and sensors by Zigbee Alliance have been adopted by the IEEE 802.15.4 standard. Zigbee Alliance includes members such as Amazon, Comcast, Huawei, Texas Instruments, Wulian, MMB Networks and many others. Zigbee Alliance was established in 2002 in order to improve and enhance existing standards for the products with the end goal of being adaptive enough to impact the lives of people in different environments. [119]

In looking at Zigbee's layers it becomes apparent that the PHY and MAC part of the structure is defined by the IEEE 802.15.4 standard, while the API, Security and Network segment is defined by Zigbee Alliance. The last layer is the Application layer and that one is left for customer use, management and implementation. In this layer different applications can be used to complete diverse tasks in the IoT and smart cities [119].

Utilization of the 802.15.4 standard consists of three different frequency bands and total of 27 channels. Channel 0 starts at 868.0 MHz to 868.6 MHz where Channel 1's center frequency is 906 MHz and has a width of 0.6 MHz. The last channel in the lower frequency range is Channel 10 with the center frequency of 924 MHz. In the higher frequency range of 2.4 GHz, the 802.15.4 standard is using 16 channels. The first channel starts with Channel 11 with 2405 MHz being the center frequency and has a width of 3 MHz. Between each channel's center frequency on 2.4 GHz range there is a 5 MHz span. The last channel has a range of 2.4 GHz and is Channel 26 with the frequency of 2480 MHz. Reaching data rates in lower band of 802.15.4 are recorded as 20 Kbps and newer versions up to Kbps.

Zigbee is an open standard and used for mostly home devices. Zigbee's ability to connect to over 65000 devices in a mesh network while obtaining low power management is a perk to the technology while also reaching a distance anywhere from 30 to 60 feet. This setup is ideal for devices such as smart lights, home hubs, heating and cooling sensors and actuators, locks and much more.

3.10 Radio Frequency Identification (RFID) Technology

Radio Frequency Identification (RFID) is another wireless communication technology that is widely used in IoT and especially in smart cities. This simple but very effective way to communicate has been around before 1950. RFID requires only a few components, a tag reader and a computer. Using radio waves, the microchip in the tag uses an antenna authentication against the reader while the reader is pulsing the signal from itself.

RFID works on a few different spectrums of frequencies one being in low frequency spectrum from 125 – 134 kHz. In high frequency spectrum RFID uses 13.56 MHz and 433, 860-960 MHz in the ultra-high frequency spectrum. Different frequencies throughout the spectrum give RFID versatility in reaching different distances [19]. For example, low frequency RFID systems can reach longer distance and can go through the obstacles such as water and metal much easier than high frequency RFID system. This occurs due to low frequencies having longer wavelengths and that can penetrate through objects better. Some applications where low frequency RFID systems are used are in animal tagging. Applications where high frequency RFID systems are used are public transportation, in hospital to trach patients and in libraries for tracking books. Ultra-high frequency RFID systems are optimal for toll roads and parking control [19].

From the paragraph before it is shown that RFID has many areas where it can be used in smart cities but are not limited to this infrastructure. In logistics as for supply chain management such as delivery, packaging and transportation a tag can be scanned during the process and which gives precise information about the load. RFID in ticketing systems are very popular, where customers can gain entrances to multiple facilities such as museums, stadiums, parking spots, cafeterias and much more. In transportation such as ticketing systems for toll roads. All these applications of RFID mentioned above are very good ways to improve smart cities and utilize cheap technologies that can do more than a single task.

3.11 Near Field Communication (NFC) Technologies

Near Field Communication (NFC) Technologies was developed in 2002 by Philips and Sony this short range half-duplex protocol is now embedded in almost every electronic device. NFC's ability to accomplish multiple tasks such as mobile payments, ticketing and data exchange are just a few of the many cases where NFC technology is being applied in real world scenarios [45].

In NFC there are three types of devices, mobile, tag and reader. These devices can only operate in specific combinations such as mobile to tag, mobile to mobile and reader to mobile but not reader to tag and vice versa. Each combination uses special communication interfaces on the RF layer where one device acts as an initiator and the other device as the target device. The spectrum supported in the NFC technology is 13.56 MHz. The data rate that the NFC can achieve is from 0.02 Mbps up to 0.4 Mbps on distances from 4 cm to 10 cm [45]. Active and passive communication modes are another asset of NFC technology. An active mode that NFC supports is when both devices are using their own power to generate fields that will be able to successfully transfer data between two devices. In the passive mode the RF field is generated by only one device which in this case is the initiator's device [45]. As NFC is a secure system, a problem appears in transition between NFC system and other systems (e.g. Using credit card through NFC system to pay for a purchase.) In this process information from NFC system need to be transferred through a third party to be evaluated and a confirmation must be given that this is where the problem could occur. The solution to this problem is to have a protected environment in the system that could store sensitive information in its memory. This system is called secure element (SE) of NFC mobile [45].

Although the initial wave of implementing NFC started slower than expected, the potential is excessive. NFC's cheap implementation, usability and convenience is making it desirable to virtually anyone. From banking, various electronic appliances, transportation, organization and mobile networks, NFC technology is being adopted by many companies across the world.

3.12 Long Range (LoRa) Technology

A lot of times architectures in different scenarios such as industries, agricultural, IoT or smart cities require a network that has longer distance and lower bandwidth. Low-power, wide-area (LPWA) technologies are just right for that. LoRa resides in technology in existence of other technologies such as SigFox and narrow band (NB)-IoT. The main difference between among these are LoRa uses unlicensed band where SigFox and narrow band (NB)-IoT use licensed [124]. LoRa is a new and upcoming technology that operates in the spectrum below 1 GHz. The major component in the LoRa technology is chirp spread spectrum modulation or also abbreviated as CSS which was used in military during 1940's to reach longer distances. "CSS trades data rate for sensitivity within a fixed channel bandwidth" [119]. In simpler words, CSS preserves low-power characteristics same as frequency-shift keying (FSK). FSK is where two signals reside with different frequencies and represent a digital signal, one frequency acts as a representation of a zero and other as one [119]. LoRa's bandwidth is from 500 KHz to 125 KHz with a data rate of 290 bps for download and 50 Kbps for upload with low energy consumption. The distance that LoRa can reach in some environments is up to 10 km.

LoRa's cheap implementation and long battery life, which can last over 10 years, gives LoRa an advantage in the integration of different networks. Using LoRa in IoT applications allows systems to stay inexpensive throughout the process. When considering LoRa for implementation there are a few things to keep in mind which are that LoRa has high latency compared to other technologies and reliability can be an issue. Some of the most common uses of LoRa are in factories and industries, smart agriculture, asset tracking and healthcare.

In conclusion to this section, the wireless technologies mentioned in this segment came a long way since its beginnings. Greater speeds, longer distances and lower power managements have been vast improvement time and time over as technology reaches new heights of achievement. Although some technologies progressed slower than the others in different fields, in the end, all of them play a major role in developing better connections and more reliable networks. Accomplishments up to this date are astonishing but there is a lot to be excited about in the future. One of example is the 5G communication that is already being heavily tested and perfected. Using higher frequencies, MIMO technology 5G can reach higher speeds than its predecessor LTE with lower latency but shorter range. This will all play a huge role in developing and planning future IoT and smart city devices and infrastructures.

4. Sensing

One of the largest aspects of any internet of things implementation, architecture, or system is the sensing. At its core, the internet of things is meant to gather data from the world around us. In the healthcare industry there are a plethora of different metrics and measurements that can be taken from the human body. The internet of things allows for real-time monitoring of bodily fluids (blood, sweat, urine, etc.) using wireless sensors that can be worn to sense and alert the patient of any life threatening or dangerous health situations. There is always a trade off with the type of sensor being used on human beings. In theory, a sensor that a patient can wear should be invisible or at least invisible to the point where it doesn't impact the actions involved with the daily life of a human being. The sensors should also be effective and unaffected by the environment that they exist in. There is a delicate balance between the human changing the performance of the sensor and the sensor impacting the movement of the human.

When more than one of these sensors are connected, they form a special type of Wireless Sensor Network (WSN) called a Wearable Body Area Network (WBAN). These WBANs can be comprised of a multitude of different types of sensors. A wearable can be worn on the wrist for photoplethysmogram (optical detection of blood volume changes). Electrocardiogram and motion sensors can be worn for rehabilitation purposes, and even simple devices like heart rate monitors can be introduced.

Cardio Sensing

Heart rate sensing or monitoring has been in use for years. Heart rate monitors are used to measure the strength and level of stress the heart is under. Traditionally, a physician would manually take your heart rate during a routine checkup using simply their hand or specially made healthcare tool. More complex monitors are integrated into full vital sign monitors, these are typically bedside in a hospital and they produce the iconic consistent beeping that we all think of. More recently, wearable heart rate sensors have become very popular in the consumer world. These sensors come in many shapes and sizes with a multitude of capabilities and applications. The new heart rate monitors can be implemented in a few common forms: wearable wrist sensor, finger sensor (pulse oximeter), chest strap sensor, and the relatively new ear sensor. In the past few years wearable wrist sensors have become very popular in the consumer electronics market. These sensors make use of an LED to make the veins in your wrist visible to the sensor which then can measure how fast the blood is pumping and in turn your heart rate. Most of these sensors come in the form of a smartwatch or fitness tracker and their capabilities range from simply giving you a real time indication of your heart rate, to tracking your position or the number of steps you have taken. These sensors are made to be as lightweight as possible, making use of mobile devices such as a cellphone as the receiver and processing unit for the data generated by this sensor.

Chest strap sensors function very similarly to the wearable wrist sensors in the sense that you wear them on your body, tight to your skin, so it can sense your heart rate. The strap itself is typically made of plastic, fabric, or elastic. The sensors themselves are either attached to or embedded in the strap. Sensors can also be embedded in something that is normally worn on the chest, like in the fabric of a sports bra or even a shirt. Traditionally, to get the best signal from the heart the sensors are somehow moistened with water or some sort of medical gel like what is used in ultrasounds. The chest strap differs from the smartwatch in exactly how it measures the heart rate, where wrist sensors use an LED, the chest straps use electrode sensors to pick up the electromagnetic pulses produced by the heart. This data is them sent using radio, usually ANT or Bluetooth to some sort of base station that can interpret and display it in beats per minute. Most often in consumer monitors this is a watch with a display that can be worn on your wrist, newer models could even make use of a smartphone or mobile device like the smartwatches can. They can also be a standalone monitor that could be placed next to a patient’s bed in a hospital.

Another cardio sensor is the pulse oximeter. The pulse oximeter was originally invented in the 1970s is a major device in the diagnosis of cardiac-related conditions. Pulse oximetry can be used by a physician to monitor not only a patient’s heart rate, but also their blood oxygen saturation, which are both critical metrics needed by emergency services. The sensors themselves are clip-like devices that are called probes. The probes are normally placed on the finger or earlobe and use light to measure the oxygen present in the blood. This information assists the physician decide whether a patient requires more oxygen during or after a surgery that uses sedation or to see how well lung medications are working.

Electrocardiogram Monitoring:

Electrocardiograms are used to show just how fast a heart is beating, whether the heart is beating regularly or abnormally, and the strength and consistency of the electrical impulses created by the heart. An electrocardiogram is used to detect many conditions or problems related to the heart such as: heart disease, myocardial ischemia, heart attacks, arrhythmia, irregular heartbeat, or heart failure. An electrocardiogram requires more than one sensor to function properly, up to 12 electrodes can be attached to the patient’s chest, arms, or legs. In an internet of things implementation of an electrocardiogram these sensors would contain wireless transmitters that would communicate with a receiver. An application running on the receiver, a local server, or in the cloud, could then identify abnormal heart activity.

Glucose-Level Monitoring:

Glucose monitoring is useful for many different applications, but it is most important for the 415 million people living today with diabetes. The internet of healthcare things can provide continuous monitoring of glucose levels while also being minimally invasive. The patients could use a wearable sensor or sensors that would transfer their health parameters via an IP based network to healthcare providers. The monitoring device is made of a blood glucose collector, some sort of smartphone or mobile device, and an IoT-enabled medical acquisition detection system to monitor the glucose level. This data can then be analyzed and used to make decisions regarding meals, medication timing, and physical activities.

Blood Pressure Monitoring:

With blood pressure being a key indicator of many health conditions or abnormalities, it is no surprise that there is network enabled blood pressure sensors. The traditional way in which blood pressure was taken was by using a blood pressure cuff. This cuff was made so that it could wrap around your arm and inflate, squeezing your arm. As the pressure was released, there would be an indicator on a dial, or a digital display, that would indicate the patient's blood pressure. An internet of things enabled blood pressure sensor would function the same way except it would be connected to some sort of wireless network in which the data can be transmitted and stored. The main difference between blood pressure monitoring and the other sensors mentioned is that due to the nature of how blood pressure is taken, there is no way to constantly monitor a patient's blood pressure. Someone must first perform the test and then the results can be sent from the sensor to a central location.

Body Temperature Monitoring:

Body temperature is one of the most consistent measurements of the human body because it remains at 37 degrees Celsius. A change in body temperature could be used to indicate homeostasis, which is the human body trying to maintain a constant state. An abnormal body temperature for a duration of time affects our body functions, which then can form create health problems. An example could be a bacterial infection. "In fact, it's one of the most common causes of change in the body temperature. Since viruses and bacteria have a hard time surviving at temperatures higher than the normal body temperature, the body detects a bacterial infection, it involuntarily increases its temperature and increases blood flow to speed up the body's defense actions to fight the infection." [75]. An internet of things temperature sensor would be the first of the embedded sensors that we discuss. All the above sensors are typically attached to the body in some way, but these body temperature sensors are made to be placed inside a human being.

Environment Sensors:

A large part of healthcare is taking preventative measures to prevent or mitigate against future problems. Internet of things implementations and systems are not limited to just looking at specific physiological signals produced by the body to determine health risks, but also environmental factors. If a user is in an environment that poses health risks, it is possible to warn them. These sensors could monitor things such as: oxygen levels in the air, air temperature, humidity percentage, radiation levels, etc. These metrics can be very useful to limit exposure to situations or environments that may cause health problems in the future.

IoT in Vehicular Networks

The sensing devices acts like human body to sense the environment, samples and collects data from different environmental parameters and transmits digitized data to wireless network modules. Sensing demonstrates its uniqueness in helping human beings to sense environment more precisely. Figure 27 shows an example of the sensor network. An overview of sensing technologies is presented as followed.

Camera sensor:

Most of the modern vehicle today has already installed some model of camera to assist the driver at some certain extent. The most popular type of camera is used for reversing moving, for helping the driver's vision at the blind spot by providing a clear image of any objects and the road behind the vehicle. According to U.S. safety regulators, all new vehicles are required to have the backup cameras starting the May 2018. Another function that the camera using for nowadays vehicle is lane departure warning (LWD) system, a progressive safety technology using a front-facing camera to monitor lane markings, that alert driver when they unintentional ride out of their lane without turning a signal. Many quality multiple cameras for building a 360- degree view of the external vehicle's environment by equipping cars with cameras at all angles support a broader picture of traffic conditions around. Three-dimensional cameras are available to represent highly detailed realistic images, giving the ability to produce the image data can be input to AI- based algorithms for object classification, and calculate the distance to them. More advanced systems require from four to six camera to augment image data with map data and satellite navigation sensor data. [80]; [116]

RADAR sensor:

RADAR stands for Radio Detection and Ranging sensors. It makes a significant contribution to the overall function of autonomous driving. The transducer sends out electromagnetic radio waves that detect objects by a receiver and measure their distance and speed in real-time. The vehicle installed both short and long-range RADAR sensor all around to take advantage of different function from each of them. While short-range (24 GHz) radar usages are lane-keeping assistance, blind-spot monitoring, and parking aids, the long-range (77 GHz) radar sensors provide more accurate and precise measurements for speed, distance, and angular resolution, make it uses for brake assistance and automatic distance control. [80][116]

Ultrasonic sensor:

Ultrasonic sensors were popular using as parking sensors for the vehicle since the 1990s at the meager cost. They are ideal for offering additional sensing capabilities to support low-speed use cases. Their range can be limited to just a few meters in most applications. Several ultrasonic sensors, which are attached on the rear and front bumpers and connected to audiovisual warning to, notify the driver about nearby objects during low-speed maneuvering. Doors may also be set up with sensors to avoid door impacts when parked. Sensors are usually deactivated when in normal driving conditions as they are confused by some weather types, mainly snow. [80][116]

Behaviors and Decision Making

In the environment constructed by [17], data acquisition was handled by a low-cost Raspberry Pi board and a USB dongle antenna. It should be noted that the dongle connected to the Raspberry Pi must be set to monitor mode so that it knows how to operate. The antenna on the USB dongle receives data wirelessly from the Wi-Fi listening devices that are strategically placed throughout the environment such that a wide area can be monitored. These listening devices are what pick up the channels that are in use in the scanned area. The listeners scan both 5 GHz and 2.4 GHz Wi-Fi channels and decapsulate the header of the packets in order to record the unique MAC addresses of all devices using the air space. One of the problems that can occur when using the MAC address for unique identification is users carrying more than one internet capable device. Packets originating from each separate MAC address would be collected and create the illusion that one user with many devices is many users. This issue is easily addressed by just giving the underlying system time to recognize that a set of MAC addresses all come on-line in very close time proximity to each other. The constant pattern gives away the fact that they all belong to the same person and so they are associated with each other. Another problem sometimes faced in an architecture like this is having overlapping records from different sensors. The data, once collected, need to be compared so that a MAC address which comes online and is detected simultaneously by multiple sensors can be recognized as a single device due to the matching timestamp. If that is done, this problem can also be avoided. Lastly, the architecture poses issues because some users could configure their devices to perform MAC spoofing. [17] explains that the effects of this behavior, however, are negligible because doing this could result in connectivity problems for the user.

Privacy also becomes a topic of concern for this sensing implementation as many vendors and app developers create tools for people to anonymize their MAC addresses. [17] elaborates on these techniques but ultimately concludes that they are not disruptive enough because to connect to a Wi-Fi network in the first place, an actual MAC address must be provided, and the tools only hide them or anonymize them up until that point in time. As mentioned in the Architecture section already, the data also is secured from a protocol standpoint. Using Transport Layer Security (TLS) over TCP/IP. The messages are sent using Message Queue Telemetry Transport (MQTT) which publishes measurements in the hierarchical structure SERVICE/ID/EVENT(/TIMESTAMP). More privacy precautions are taken and discussed by [17] such as an irreversible hash MD-5 function and salting the MAC addresses all at the sensor level.

In total, the architecture used nine sensors over the course of one year. The sensors generated 1 CSV file every 15 minutes, but by the end of the analysis, 246,000 files would be created. This data collected however, is gathered from any person who entered the range and used the university's wireless network. Additionally, [17] states that 4,000 different people walk through the Telecommunications Engineering School of Polytechnic University of Madrid daily. This is a very interesting thought when comparing the source of this data to that of the data [99]. The home monitoring system that allows doctors to yield rich information with ease from the internet connected devices. The number of sensors required for this type of system is dependent on the user's home but [99] states that 80 sensors were considered in its research and they used a wireless IoT sensor kit made up of different specific sensing devices. The devices selected in this scenario also leverage the existing 802.11 Wi-Fi network that users have in their homes and they only need to be installed without deploying a dedicated wireless network. The types of sensors that this architecture utilizes are much more complex than those used in [99] as the behaviors which are being monitored are also more complex.

The behaviors that the system currently monitors are collected with 5 different types of sensors included in the IoT kit used. The first one is a Passive InfraRed (PIR) sensor for detecting motion and is also capable of measuring how many people are in its vicinity. The second type are magnetic contact sensors for detecting whether something is open or closed. [99] explains that this sensor is good for doors, drawers, and medical cabinets. Next is the bed occupancy sensor which not only is useful for what the name implies (bed occupancy) but for collecting sleep data which can be used to find patterns in a user's behavior while sleeping. This is done by installing a pressure-sensitive resistive pad under the user's mattress whose signals are collected by a module connected to the bed frame. Since it is normal for people to occupy their own bed when not actually sleeping, the sensors have been set to filter out short-term occupancy because these small time periods do not yield any data related to sleep activity. The architecture also contains a chair occupancy sensor. This mechanism implements the same pressure-sensing pad as the bed occupancy sensor. Finally, a toilet presence sensor is deployed to monitor the usage of the toilet. An InfraRed sensor coupled with an InfraRed illuminator and photodetector provide very selective monitoring of close interactions. [99] states that this sensor must be placed near the toilet to provide the highest quality data possible to the system

Something that the author of IoT-Based Home Monitoring considered to be very important was the power profiling of the IoT sensors. They mention that with the growing popularity and interest in Wi-Fi enabled sensors, we are required to think about how these devices can become more cost-effective so that patients and practitioners see value in deploying these systems. Power profiling is important because the devices used take advantage of protocol that support high bandwidth which consequently leads to higher power consumption. The following table summarizes the different power demands for devices used in [99]:

Transmitting the data over Wi-Fi is shown to be the biggest consumer of power in this environment. To mitigate the relatively large amounts of power consumed by undergoing this process, the sensors have been configured to use burst-based data transmittance. This essentially just means that data will be grouped into bursts before being transmitted. This strategy according to [99] will reduce overhead compared to transmitting data now which the sensor gathers it.

doi:10.20944/preprints201912.0276.v1

Table 6. Current consumption under different conditions for different sensing devices

Condition	Current Consumption
Wi-Fi Receive and Network Scan	80 mA
Wi-Fi Transmit	290 mA (peak)
Wakeup and Event Logging:	
• Bed, chair, contact	2 mA
• PIR, toilet	14 mA
Sleep (power save)	12 uA

The next sensor platform that we will go into detail over deviates a bit from what we have discussed thus far; Especially in terms of the sensing/data acquisition function of this architecture. The environment is at a museum and seeks to monitor the behavior of attendants based on their paths through the exhibits and their interactions with the Points of Interest. The author in [68] refers to IoT as a network of connected physical objects, in which sensors and actuators are seamlessly embedded in physical environments, and information is shared across platforms to develop a common operating picture. This definition of IoT aligns quite well with the architectures we have discussed so far and manages to encapsulate other architectures we have not. Conveniently, [68] contains a reference to research done by Evangelatos et. al. [54] which elaborates on a wireless IoT network that is most relevant to the IoT network in [68]. This network is fitted with wireless sensors and actuator nodes that run on an IPv6 6LoWPAN network. This will allow devices to connect directly to the internet. What happens to the traffic after it leaves the sensor will be discussed further in the systems section? The sensor nodes in [54] use technologies like NFC, Bluetooth, ZigBee, and 6LoWPAN to detect behaviors and actions of users in an office building such that an adjustable and comfortable work environment can be created based on the outdoors conditions and specific users. The architecture contains a dedicated Wireless Sensor Network (WSN) using Waspmotes by Libelium to identify and track users. These sensors are built for developers as they support ZigBee, Wi-Fi, Bluetooth, NFC/RFID and GSM/GPRS interfaces. In [68], the sensor and actuator nodes are not the only means by which the system collects user behaviors. Museum attendees are prompted for preferences when they first arrive at an exhibit at a check-in station. This information personalizes their experience by showing them different content. Lastly, user's online behavior is collected and considered when determining what content to display to them and what path to take through the museum.

IoT in Learning Environments

Definition

In order to best understand the pertinence of sensors to any Internet of Things system and architecture, it is key to clarify what defines a sensor. It is of the authors' opinions that a sensor is best defined as an object with the purpose of collecting information. Serdaroglu and Baydere best denote the device as one that is capable of data acquisition and is often embedded within a given physical phenomena [120]. It is noteworthy that while a traditional sensor utilizes mechanisms to collect physical data, the term lends itself to a more abstract definition within an Internet of Things system.

Purpose

Sensing in any Internet of Things environment is paramount to the success of the system, and truly redefines the abilities of a given system. Through the utilization of the wireless communication methods, varying types of sensors can transfer collected information to a separate device within the IoT system for storage and analysis. The targeted learning environments of existing IoT systems vary in shape, size, and general activity. It is due to this that each system's use of sensors varies.

Requirements and Features

Sensors within an IoT context are required to have certain capabilities in order to function as designed. Were sensors across the board to be absent of any commonality, it would be increasingly difficult to manage the information gathering process within an IoT environment.

1. Unique Identification

Most, if not all Internet of Things applications require more than one device geared towards collecting data. For this reason, it must be ensured that each device that collects data (and therefore each sensor) contains a means of uniquely identifying itself among the other devices connected to the network [106]. This ensures that any collected data is not overwritten, duplicated, or incorrectly stored when sent to the information storage systems. Identification is most often achieved through alphanumeric or numeric codes registered to each sensor or device [106].

2. Network Integration

In order to properly function within an IoT environment, sensors are required to integrate into some form of network. This network is used as a means of information exchange and functions as the backbone to the interconnectivity of IoT devices. In addition to the exchange of information, this network also allows the sensors to dynamically discover other devices such as other sensors and information collectors [106].

3. Power Consumption

Each device within a system fundamentally requires energy to actively function. Sensors are no exception to this rule, and the level of power consumption among varying types of sensors is a noteworthy requirement when planning and designing an Internet of Things system.

4. Device Interaction

One of the key features of an Internet of Things environment is the configuration of many devices on a single network. With this feature, it is required that each device connected to the network has the capability to safely and routinely interact with other devices. This interaction must also not be limited to devices of identical functionality, meaning that sensors should also be able to communicate to devices beyond other sensors.

Types of Sensors

Sensors that meet the requirements found in sub-section (B) are discussed below based on functionality.

1. Infrared Emission Sensor

The infrared sensor (IR) has the ability to detect infrared waves that are invisible to the human eye. In many cases, these sensors also can emit IR light in addition to detecting [114]. The use of IR sensors in an Internet of Things learning environment enables the system to detect various objects.

2. Barcode Scanning

A barcode scanner has the ability to read either one- or two-dimensional barcodes. The use of barcodes in an Internet of Things context enables the system to create records of various objects.

3. Radio Sensors

Various sensors utilize radios to detect varying frequencies. These frequencies can represent wireless communication between devices external to the IoT network.

Data Capturing and Transfer

Based on the type of sensors used, as well as the overall implementation plan for the given Internet of Things system, various sensors by themselves may not be able to transfer the data collected to other sink devices in the system. Among the most common sensors available for general use, microchip devices like the Raspberry Pi and Arduino bring functionality to certain sensors. These open micro-controllers offer an easy to use development environment, which presents them as a common choice for newly developed Internet of Things systems. The controllers can be custom programmed to enable a wide variety of instructions and can be developed to meet the requirements of data collection and transfer within an IoT system.

Paradigm Specific Applications

With the abundance of use cases for the Internet of Things architecture, the following points detail technologies integrated into various learning environments as a means of collecting data.

1. RFID Tag Reading

Student identification cards have existed for decades as a means of verifying a student's status and attendance at the respective school. More recent identification cards have included magnetic stripes to interface with various school devices like cafeteria registers and automated building door locks. Many cards are now embedded with electromagnetic tags that passively provide electronic information when in appropriate contact with an interrogating radio frequency [53]. This provides the card a means of interfacing with RFID scanners.

2. Pressure Plate Detection

Many learning environments offer open computer laboratory spaces for patrons. As these spaces are frequently in high use, many include "smart chairs" that detect whether weight is applied to a pressure plate within the seat [53]. This provides information as to how many chairs within a computer laboratory are currently occupied.

3. Exam Pad Success Tracker

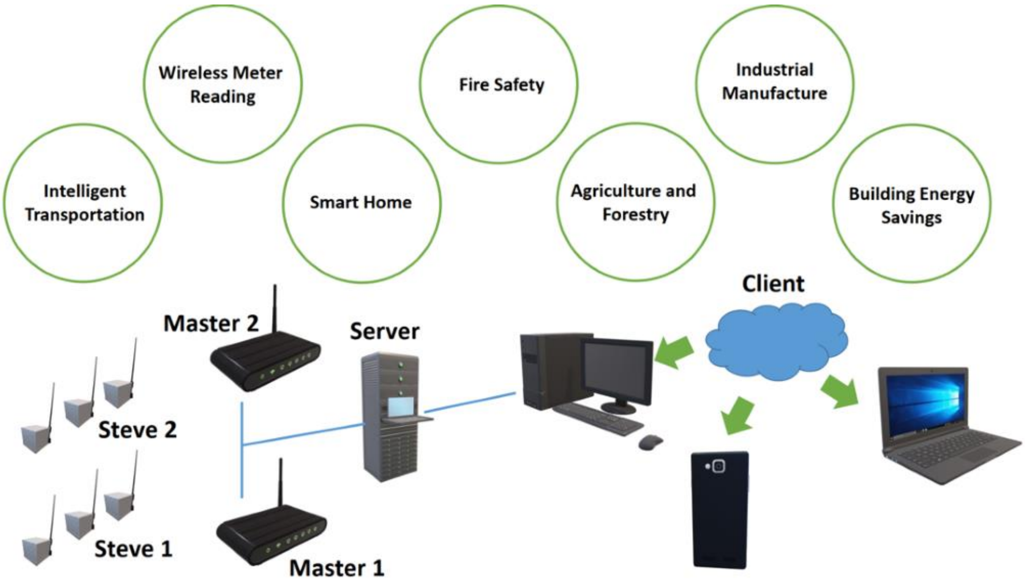


Figure 17. Client-LMS Interaction (ChinaPCB, 2017)

Students at a university in India were provided tablets called "Exam Pads" which monitored academic performance in examinations completed using the tablet. The information was delivered using a pre-existing internet connection as a backbone and delivered data to the learning management system which could complete holistic analysis from a plethora of students' data [112]. Provided in Figure 3 is an example visualization of a multiple-client-supported IoT system that displays the interaction between things, sensors, and the database management system for the Internet of Things learning environment.

IoT in Mining

While mining has existed for centuries, the ever-looming danger of injury or death of a human has always remained constant. Whether it may be a cave collapse or simply by human error, the result is always a risky one. It is now within this new generation that IoT devices are being introduced as a method of preventing critical errors in the form of network sensors.

Regardless of cave type, implementing sensors in cave systems not only helps map out areas of the cave, but can offer new and advanced features as well. One of the most common types of sensor in the mining industry is hazardous gas detection. These types of sensors are not like simple carbon monoxide detectors in an average American household as the ones used in cave systems can detect extremely slight hints of poisonous gas, type of gas, and even estimate areas in which pockets of gas may be. This helps in preventing a nearby miner to accidently enter or mine in the dangerous area.

In relation to gas, sensors placed in hazardous areas of a mine can also differentiate between gas particles and levels of carbon monoxide/dioxide to indicate whether there is an active fire present in the area. For this purpose, various semiconductors are used and are generally programmed to alert of a fire if the ratio of ethylene and carbon monoxide in the air has a ratio of 100:1. By using this specific rule in the sensor, it allows for the onboard computer to filter out false positives and save the workers both time and money from having to check the area out.

In the new generation of IoT, simple gas sensors have become so much more advanced to the point of linking up with other sensors to form an underground network. In this network, workers wear trackers when in the mine so that managers can use the network to find exactly where they are located. These sensors also offer advanced precautionary scans on a timely basis to establish safe, risky, and restricted zones in and throughout the mine. If a worker were to stumble into a restricted area, an alert will go off on both the workers and managers trackers to notify them of imminent danger. This tracking system is also implemented on mining vehicles. If a vehicle is approaching a worker and neither parties know of the other, a proximity alarm will go off warning both workers that the other is near. These network alarms also act as an S.O.S beacon if a worker is trapped or in need of help. The sensors will then geolocate where the individual is in the mine and send their location to an above ground source which can then handle the problem accordingly.

In the most recent years, biotechnology has also been implemented in the trackers of miners. This kind of technology is used to detect for various incidents that may happen when in a mine. One important feature of this is immobility detection. If a miner were to become unconscious or stand still for a length of time, an alert would be sent to the miner to move. If the miner has not moved within a period, a much wider alert would be sent out to above ground staff and or first responders reporting their location in the mine. Some sensors also provide vital technology that can relay vital signs of an individual back to above ground sources to indicate the miner’s current health conditions such as BPM.

Another type of detection implemented in these trackers act as a form of speedometers. These are used in mines to help detect the rapid change of movement or speed that a miner might make. The most important reason for having this feature is to help detect when and if a miner goes into freefall from possibly falling off an edge or a rope. Once this feature is triggered, an emergency alert will be sent to above ground staff indicating when and where the fall occurred. In more of a professional approach, these features in sensors can be used by managers and staff to calculate the speed of underground vehicles, estimate arrival times to sites, reduce radio communications, prevent collisions, and to better improve traffic conditions underground.

While safety always comes first, protecting miners isn’t the only thing that underground sensors can do. Telstra Mining Services recently deployed several sensors underground in Queensland to create a privately-owned LTE network for the Cannington mine. With this type of network installed, the sensors are very fluid by default and allows for the manipulation of the private network to eventually upgrade to the 5G protocol, increase or decrease the radius without any down time. Implementing LTE networks in systems like these also remove the issue of radio communication. Often, cave walls may contain heavy elements such as lead that may jam or prevent radio signals from being sent or received. In an LTE network, this issue is solved simply by traveling from node to node around the cave to get to its destination. This prevents any possible communications between vehicles or workers to be interrupted and helps sustain a stable work environment.

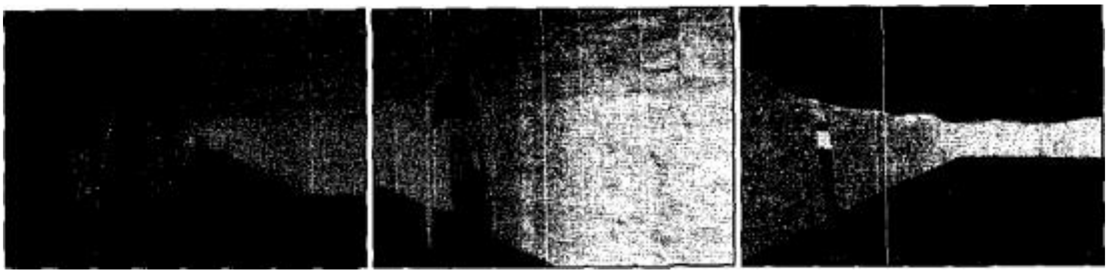


Figure 18. Using volumetric mapping to paint layouts of cave systems

With the advent of drones and remote controllable technologies, we have now opened a new door to the possibilities that sensors can play a role in. For example, ever since the dawn of time, humans have gone spelunking or explored cave systems whether for leisure or for business. More often than none, people have become trapped, injured, or even died from cave exploration. In today's world, drones and sensors have become one and are used in unexplored underground systems with the aid of 3-dimensional volumetric mapping not only to help create a map of the system, but also to locate areas where rock is loose, indicate the existence of toxic gas, and overall document whether the cave is safe or stable enough to enter [25]. Figure 7 below demonstrates a sensor over a short period of time using volumetric mapping to paint a 3-dimensional image.

IoT in Energy Systems

Smart Meters

According to [7], "A smart meter is an electronic device that records consumption of electric energy and communicates the information to the electricity supplier for monitoring and billing". Smart meters are excellent and cutting-edge tools designed to be mainstream solutions to monitor customer electricity usage. The readings given from these meters are then used to complete a customer's usage bill and calculate their total usage. Smart meters can be implemented to monitor all utilities including gas, water, and electricity usage.

Smart meters are extremely useful in replacing the current implementation. Smart meters can eliminate the need to physically check meters. They have the ability to send their readings wirelessly [138] and can notify suppliers of use instantaneously. This makes them very effective in reducing time wasted in taking manual readings and saves the suppler money. A consequence of giving the supplier faster readings means that customers can have very accurate monthly estimates. When using an online account, a customer can view their monthly readings and the supplier can keep them up to date faster. This allows customers to anticipate their monthly expenditures and promotes customers to save more electricity as their bill is constantly shown to them. This could lead to an improved environmental impact and encourage customers to reduce their electricity usage by being more conscious of it [138]. Currently, it does not cost anything to have your meter upgraded to a smart meter depending on the supplier you are with. It will, however, be reflected on your usage bill [138]. Another side effect of constant monitoring can lead to a health and safety improvement. If the customer monitors their usage levels regularly and notices an unexpected spike, they can check for leaks quickly and increase their chances of preventing an issue.

Some first-generation smart meters lose their functionality when you switch suppliers [138]. This is an example of some of the burden that will be placed on new technology like all others. Manual meters have had many years to be developed and perfected while smart meters are still in the trial period. Although the technology is new, because it is software-defined, it can be upgraded without installing a new smart meter. This allows for issues to be addressed remotely and should be fixed faster than someone manually replacing the meter. Some people may want to wait until the technology is improved, however, depending on the use case, this technology could prove more beneficial than annoying. A potentially overlooked con of smart meters is privacy. There will be large amounts of data collected from smart meters and that data will be stored. Energy companies will have the responsibility of accommodating for large amounts of data and that could fall on the customer's bill. They could also risk security vulnerability and become a potential target for hackers. This could also cause an issue with the smart meters themselves being connected to the user's home networks and vulnerable to a network attack.

Currently, in the United States, there are 70 million smart meters installed. This is a staggering number, but the technology was invented in 2006 [73]. Each state has its own policies regarding smart meters [73]. Much of this is due to how the population of that state perceived smart meters. Some states have a larger rollout than others because of this. Northern California has the smartest meters installed at 5 million units [73]. These meters send data on an hourly basis and eliminate the need for the company to send employees to manually check them [73].

With 70 million smart meters currently installed in America, it's not a question of should we use smart meters anymore. They are already a daily part of our lives. Software updates, privacy improvements and accurate readings account for some of the controversial topics of smart meters. Overall, they eliminate the need for manual readings, allow customers to be more conscious of their energy consumption, and appear to be here to stay.

Smart Sensors

As mentioned in the Smart Meters section, smart meters make up a large portion of IoT sensors. They can be used for gas, electric, water and almost anything else that can be electrically measured. Another part of IoT in energy is the smart sensors themselves. Whether this be devices installed on the smart grid, sensors housed inside home devices or smart meters sending data to and from utility companies, everything comes with a sensor that company ultimately want to adhere to the following requirements: Low cost, Physically small, Wireless, Self-identification, Very low power, Robust, Self-diagnostic, Self-healing, Self-calibrating, Data pre-processing [130]. Smart sensors take a real-world variable and use software processing to turn that into a digital data stream for transmission to a gateway [130]. They use a series of algorithms to achieve this and attempt to process as much data as possible before sending it to the network to reduce the amount of traffic on the network [130].

Smart photoelectric sensors can detect patterns in an objects' structure around them [130]. This allows them to increase their processing throughput and reduce load on the central processor [130]. Today, Manufacturers have increased their flexibility so that smart sensors can be remotely programmed [130]. This provides a huge reduction in the amount of physical labor that comes with installing and troubleshooting these devices. Companies can now have a dedicated team of remote workers to address sensor issues without using the time and manpower to fix them in person. Traditionally, feedback from these smart sensors has been hampered by problems relating to system noise, signal attenuation, and response dynamics [130]. New sensors can self-calibrate to accurately and reliably determine the correct parameters for operation [130]. These sensors are also durable as they are small and can be installed in harsh weather environments with their IP67 and IP69K seal rating [130].

As with most RF technology and IoT equipment, the cons continue to be RF exposure and privacy concerns. Having all devices on a localized network creates more points of intrusion. Hackers have more opportunity to bypass network firewalls and gain access remotely through these devices. Security needs to be a top priority when designing and implementing these devices in the field because of this. The other issue with IoT sensors is RF radiation. The sensors described in the Tech Briefs article Smart Sensor Technology for IoT describe sensors that operate on an "ultra-low-power MSP430". The question remains, however; when is too much RF exposure and what levels are safe for humans?

Currently, there are countless types of sensors and devices available for use in real-world applications. According to [5], these sensors and actuators cover a spectrum of protocols and technical requirements including machine vision, optical ambient light, position, presence, proximity, motion, velocity displacement, humidity, moisture, acoustic, sound, vibration, chemical, gas, flow, force, load, torque, strain, pressure, leaks, levels, electric, magnetic, acceleration and tilt. There are a wide variety of IoT sensors and if it's mechanically measurable, there is probably a sensor for it. With future improvements and further research these devices will become smarter, faster, more durable, and longer lasting on small amounts of energy.

Smart sensors compose a huge variety of devices. If you can measure something electronically, there is probably a smart sensor for it. Sensors continue to get smaller, more energy-efficient, stronger and can be engineered for harsh environments using sealing and water resistance techniques. Concerns regarding privacy and RF frequency exposure are still widely prevalent for this new technology. Further research and long-term testing should be conducted on RF exposure to conclude the level of harm it causes to our bodies. Privacy and network security are huge factors in IoT, and smart sensors are no different. The utmost caution needs to be taken when developing these devices and deploying them into the consumer marketplace. Despite these cautionary tales, smart sensors are in mass-deployment and here to stay.

Power Management Techniques

With the rise in popularity of IoT and devices that utilize it effectively, designers are focused now more than ever on creating devices that adhere to industry requirements. A huge advantage in IoT is having devices that can go long amounts of time on small charges. Often, IoT devices are in remote settings or environments that do not allow for wired connections. A big part of IoT's appeal is being able to wirelessly communicate between devices without the need to run cables and complicate infrastructure setup. This means that IoT devices need to go long amounts of time without receiving electricity directly from an outlet or remote power source. IoT sensor devices are usually small in size making it more difficult to pack large batteries. They also often need to be weatherproof which usually restricts the sensor's body even more. Design considerations usually include "major system elements such as the microcontroller (MCU), wireless interface, sensor and system power management" [2]. A good example of a device that requires these specifications is a wireless sensor node.

Most MCU need to be extremely energy efficient. Some devices need to be able to go months or a year to be effective. IoT in farming is a good example of a device that needs to be able to last if possible, to be effective. These devices should ideally last a year or crop rotation so as not to cause too much hassle by is considered requiring battery replacements. The computational requirements of a wireless sensor likely will require 32-bit or 8-bit MCU [2]. Even though the computational requirement of the MCU is high, the power requirement remains low. This proposes a big engineering challenge for designers and results in many optimizations and techniques to get the most charge out of a battery possible.

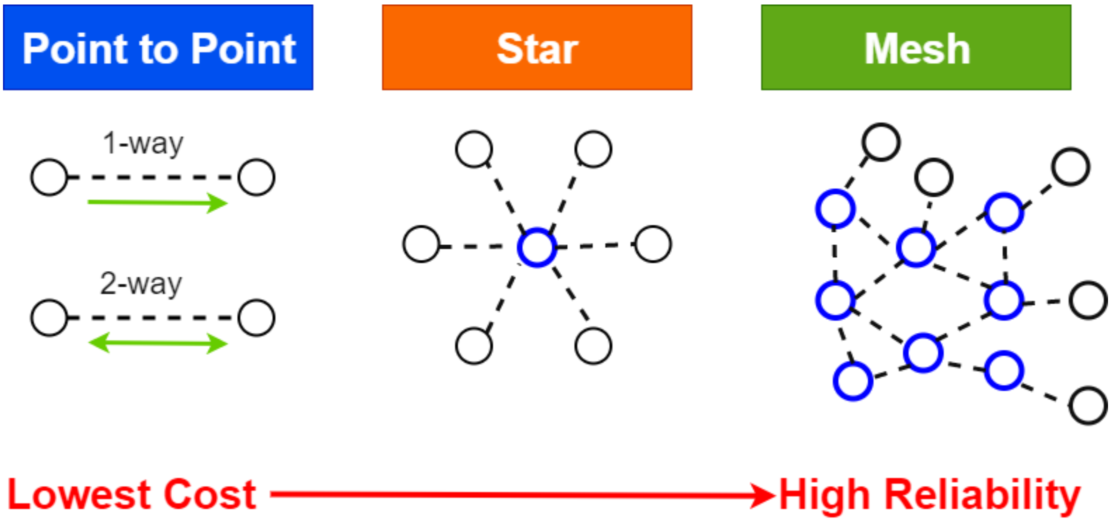


Figure 19. Typical Sensor Network Layouts

Regarding wireless connectivity, the network topology and choice of protocols will have a large effect on the device's ability to sustain the battery for extended periods of time [2]. In most cases point-to-point links would yield the lowest demand from the battery, however, this limit where and how the sensor can be deployed [2]. The following figure compares the lowest cost networks against the reliability and scalability of the network topology.

As we can see from the diagram, point to point networks are the lowest cost and possibly the best on battery but mesh networks provide the best reliability and can be sustainable if implemented correctly. Mesh networks do take a large toll on battery life but may be the best option in a self-healing network [2]. Star networks are a nice step up from point-to-point, however, they add a lot of complexity to the protocol and increase the amount of RF traffic and system power [2].

Smart City Sensing

What constitutes a city to be a smart city and what is the difference between a smart and a "ordinary" city. This is the question that a lot of people ask and remain unclear about. This concern is valid because what constitutes a smart city is ever evolving. The Journal of Urban Technology published an article about Smart Cities in Europe [36] and stated that there is not a one definition that defines a smart city. Some have tried to put this concept in terms of a cities' communication infrastructure. Even though communication is an important part of any smart city does not include everything. This definition was introduced in 1990's when technology was heavily under development. In a more recent study from Vienna University of Technology the researchers had a little bit different perspective on the definition. They thought that smart cities should not be tied only to communication infrastructure but also to smart mobility, smart economy, smart environment, smart living and smart governance. The researchers were basing their definition on different theories such as reginal competitiveness, transport, natural resources, social capital and quality of life to name a few. [36]

One characteristic of every smart city that allows everything else to be part of it, are the sensors. Sensors are a foundation of the ecosystem in the smart city because they provide valuable information. Types of information that can be received is only limited by what sensor is capable of. Information gathered from sensors later get distributed to different systems, databases and places where the data can be stored, queried, studied and acted upon. This is very important because it can give autonomy to a smart city by allowing computers can make a decision without human interactions or supervision. A good example for this would be having a traffic jams on the intersection from one side where other side does not have any. In this situation sensors would be able to detect congestion and let the green light last longer on the side with more vehicles. As sensors in smart cities is a very broad topic this paper will focus on more critical infrastructures such as water systems, power and energy systems, transportation and first responders' systems.

One of the most critical pieces of infrastructure in every city smart or conventional is water supply. The ability to have information about water levers and water quality allows better displacement of water itself and actions that need to be taken to bring water to the right chemical amounts almost instantly. One example that was presented in an article about "Smart water grid: the future water management platform" by Seung Won Lee is the need of water in different parts of the USA during the year. During different periods in a year in the USA western states may have drought problem where states in the Midwest have flooding problem. A solution to this problem would be making a smart water grid where massive amounts of water can be moved from the states that have floods to the states that need water. [84]

Another important part of the infrastructure is power and energy systems. These systems are very complex and require a lot of care. Some of the main goals of different smart energy systems is be able to control and predict usage of energy throughout the year and to be able react upon that, such as to displace energy from low areas of usage to high usage areas, plan for new power grids and give customers almost if not a real time insight of their usage of different energy systems. This was resolved by smart meters that allow energy companies to have accurate database of its users and their consumptions. Some of the devices such as smart electricity meter and gas meter are presented in Figure 20. below.

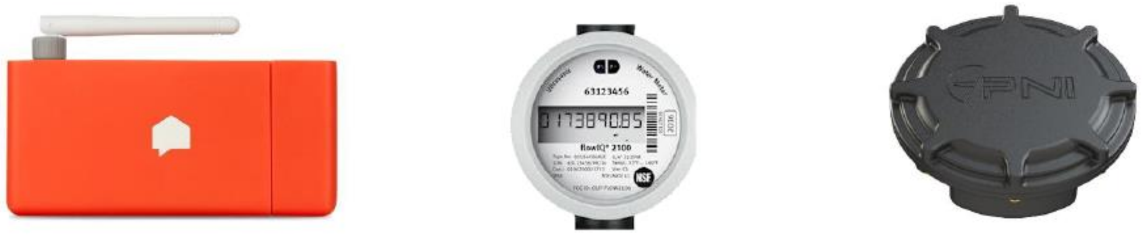


Figure 20. Smart energy meter (The Sense Home Energy Monitor nd), Smart water meter (Smart water meters nd), Smart parking sensors (PlacePod Smart Parking Sensor nd).

As talked about previously in the paper as an example, usage of sensors in transportation can help in traffic congestion but is not limited to that. Smart parking systems throughout the world have shown better displacement of parking spots and parking garages. Being able to see which garage or street an empty parking spot has is not only beneficial to a driver but to the environment where they do not have to drive around blocks, unnecessarily polluting cities even more. Collision detections system can be useful where drivers can be alerted to an accident and avoid the road that it is on. Smart parking sensor is presented in Figure 20.

When first responders are call upon the single most important variable is the time that they need to respond to a problem or an incident. This variable could be deciding between life and death situations and that is very important to detect problems if possible, even before they happen. As massive shootings are a problem throughout schools not only in USA but in the world, a smart system where this can be detected before it even happens would help solve this problem. This system can be consisted of different camera sensors where an active shooter can be detected before they are in the building. Upon having an alert of an active shooter, the system can send information to local police departments, alert other schools nearby to be advised and act such as by locking the external doors. This is just one of the examples where smart infrastructures can be critical and this is where a variety of sensors come in place to prevent or detect incidents. Other sensors that can help first responders such as smoke detector sensor, CO sensors and doorbell sensor s which will be discussed later in this paper

Sensing in Smart Homes

One proponent that fuels the idea of the smart home initiative would be implications on the energy system. The culture of today’s society is becoming more and more conscious of the affect that industry and consumerism has on our world as such conservation and efficiency of energy is leading today’s research and technology.[41] Coinciding with the smart home would be the internet of things (IoT), as stated by Yang, Lee and Lee [143], “IoT-enabled house equipment allows for a smart home to be more intelligent, remote controllable, and interconnected.” [139]

Smart home technologies (SHTs) consist of functional home appliances such as refrigerators, televisions, water systems, air temperature regulation systems, lighting systems and dish washers but also include devices that provide feedback, connectivity and control to the consumer such sensors/monitors (for changes in humidity, light, motion and temperature) , network devices that could provide remote control capabilities as well as automation as directed by user. The user has further ease of use by having control features assessible from their smart phone, computer, tablet or other devices. Due to the diversity of SHTs they can be configured typically wirelessly to provide the user with a home functioning optimally to meet their needs. [41] Artificial intelligence is another component of emerging smart home technology, Amazon created “Alexa” an intelligent personal assistant that can be installed in a variety of products providing services such as searches, shopping and schedules. Apple is creating a similar AI support called “Apple HomeKit,” which is intended to provide voice support in smart home technologies. [139] Equipment added to devices to make them "smart" would include, in addition to sensors, cellular communication, NFC, WiFi and Bluetooth. [143]

Consumers using SHTs benefit from increased security, energy management and conservation, accessibility to leisure and entertainment services and even living assistance and independence when a healthcare need arises. [41] Automation is the critical function of smart technologies as it is the replacement actions previously carried out by the human. [139] By the year 2022 the market for smart homes is expected to grow globally to USD 119.26 billion. Companies such as Google, Samsung Electronics and Amazon are joining the endeavor of smart homes and pushing the market forward. [139]

Barriers that prevent consumers from jumping on board with SHTs might be fear for privacy, lack of awareness of technologies, cost concerns and upon implementation lack of interworking technologies and systems. [41] Additionally, Yang et al [84] notes, "The largest barrier is due to a lack of technology to establish the infrastructure of a smart home, "and furthermore indicated, "technological or engineering perspectives on smart homes have failed to interpret potential users' actual needs from a smart home." Considering this needed infrastructure, a change in the technical standard is necessary as satellites are too costly and transmissions among electronic devices are limited. [139] A possible downfall to censorship provided through the use of sensors in smart home technologies would be the back door hidden with in most devices that allow for third parties to gather data on users without their knowledge, for example tracking purchases, logging personality traits and even user identification which is a threat to privacy and security. [84]

Wilson, Hargreaves and Hauxwell-Baldwin [139] summarize in their research article, benefits and risks of smart home technologies, which they based from research gathered within countries of the European Union, that the outlook for the SHTs market is positive, with potential consumers seeing value in the convenience of SHTs but note that time will tell if design and usage of SHTs have a long term impact on energy efficiency and further note caution regarding the autonomy and independence of home technologies in light of the risk to privacy and data security.

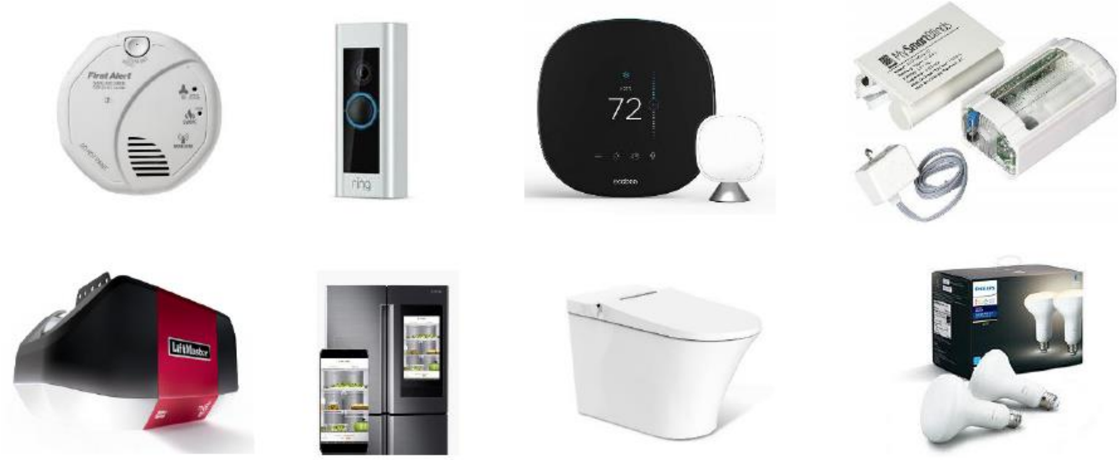


Figure 21. Top row: Smoke Detector and CO Alarm (Albright 2015), Video Doorbell (Video Doorbell Pro nd), Smart Thermostat (SmartThermostat nd), Smart Blinds (MySmartBlinds nd). Bottom row: Smart Garage Door Opener (Smart Garage Door Openers nd), Smart Refrigerators (Samsung Smart Refrigerator nd), Smart Toilet (Intelligent Toilets & Seats nd), Smart Lights (Smart Bulbs | Philips Hue nd).

Sensors are a crucial technological aspect of smart home devices. Sensors are the component that collects and analyses data which then is used to enhance the quality of the user experience. [143] An example of which might be blinds automatically closing during the brightest times of the day to conserve the energy used in keeping the home cool yet being open to allow for natural lighting during dusk and dawn when this is not a concern. Another would be the use of biometric data, such as the fingerprint, which is used to verify user ownership rather than having the user remember a code or password. The system must identify the pattern of the fingerprint by measuring the distances among skin fissures and as such determine user authenticity. Some of the sensors in smart homes are shown in Figure 3. below. Regardless of the device it must always can sense elements of the environment they are calibrated to measure and then communication the data to then direct the implementation of the automated action, this communication also allows for machine learning. [143] Masoud, Jaradat, Manasrah and Jannoud [92] provide additional insight in their article, Sensors of Smart Devices in the Internet of Everything (IoE) Era: Big Opportunities and Massive Doubts, "a fridge with an embedded processor is not smart until it has the ability to communicate with people, other fridges, and supermarkets to order missing items. Moreover, it should select from different supermarkets to buy the items with price offers. This smartness came out from data communication over the Internet."

There are a variety of sensors that today we often take for granted. Power sensors can be set to turn an appliance off after a duration of nonuse. An accelerometer senses the user's orientation and changes and rotates the viewing screening accordingly. Motion sensors can be classified into three different methods of detection, accelerometer, magnetometer and gyroscope. [143]

5. Systems

5.1 IoT in Health

5.1.1 Environment sensing

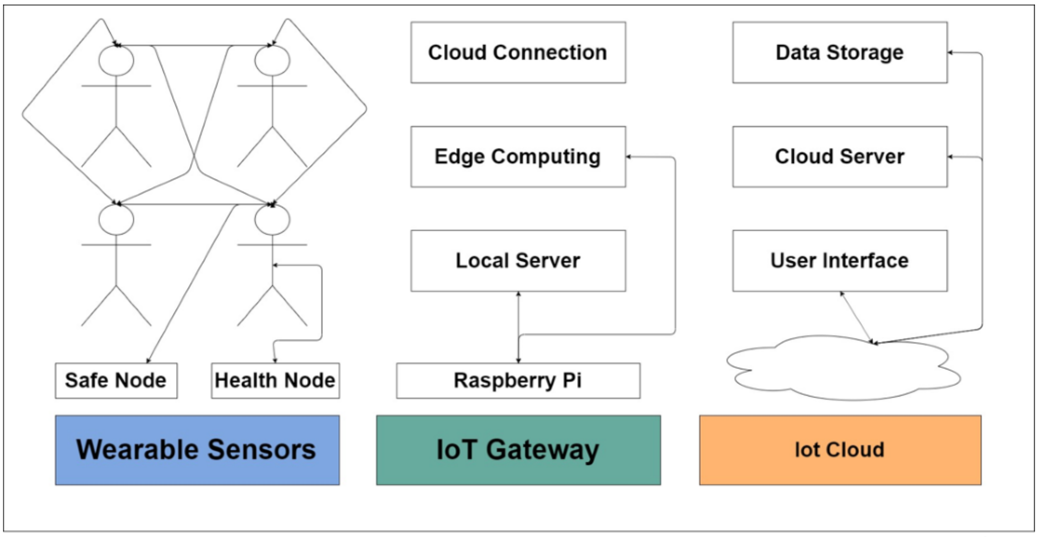


Figure 22. Architecture of the proposed WBAN

IoT systems can be heavily used to monitor a human's surrounding environment. A wireless body area network can be used to monitor the temperature, humidity, or even ultraviolet light levels to ensure the safety of the person working in their environment. Safety and health are key when thinking of an industrial workplace, especially for those that could put a person in a dangerous environment. To prevent workers from exposing themselves to hazardous situations, some of the physiological sensors mentioned above can be used. A person's body temperature and heart rate are good point-in-time indicators of a health condition or abnormality. The system also proposes a safety sensor, monitoring things like the strength of harmful UV rays or the carbon dioxide content of the air. Both ultraviolet rays and carbon dioxide are known causes of cancerous tumors and being able to detect the conditions that cause them goes a long way in preventing patients from developing these tumors. The figure 34 shows the architecture of the proposed wireless body area network safety and security system. In this implementation, each safety node is equipped with a power management unit, a LoRa module, a microcontroller with Bluetooth, and four actual sensors. The whole node draws power from a rechargeable battery providing a constant 3.3V to the system. The RFM95 LoRa module was chosen as it is a low power and long-range transceiver and will have no issue connecting to the remote gateway. The four environmental sensors chosen were an external temperature sensor, a relative humidity sensor, a carbon dioxide sensor, and an ultraviolet ray sensor. The health node is comprised of a power management unit, a microcontroller with Bluetooth, the heart rate sensor, body temperature sensor, as well as another rechargeable battery supplying the same 3.3V. All the data being collected from the health node is sent to the safe node using Bluetooth and then to the gateway. A visual representation of the system is shown in the figure 23.

The edge gateway chosen was a Raspberry Pi 3 along with a wireless module, and a power supply. Raspberry Pi's ship running Raspbian, which is an open source Linux distribution that supports many different common programming languages like Python, C, C++, and Java. The Raspberry Pi is a good option for this internet of things deployment because of its low power usage, only requiring 5V at 2.5 amps easily supplied by the portable power bank. The low power consumption allows for the Raspberry Pi to be easily moved from place to place, if the environment changes or the system needs to be moved for any reason. Finally, another LoRa module is added to the Raspberry Pi to allow communication between the gateway and the safe node. The data collected from the system can be consolidated, processed, and analyzed in a cloud solution. This system utilized Digital Ocean as a cloud service provider. This cloud solution provided a system using Ubuntu server 16.04.5 that ran a secure web page to access the data, as well as a MySQL database to store this data.

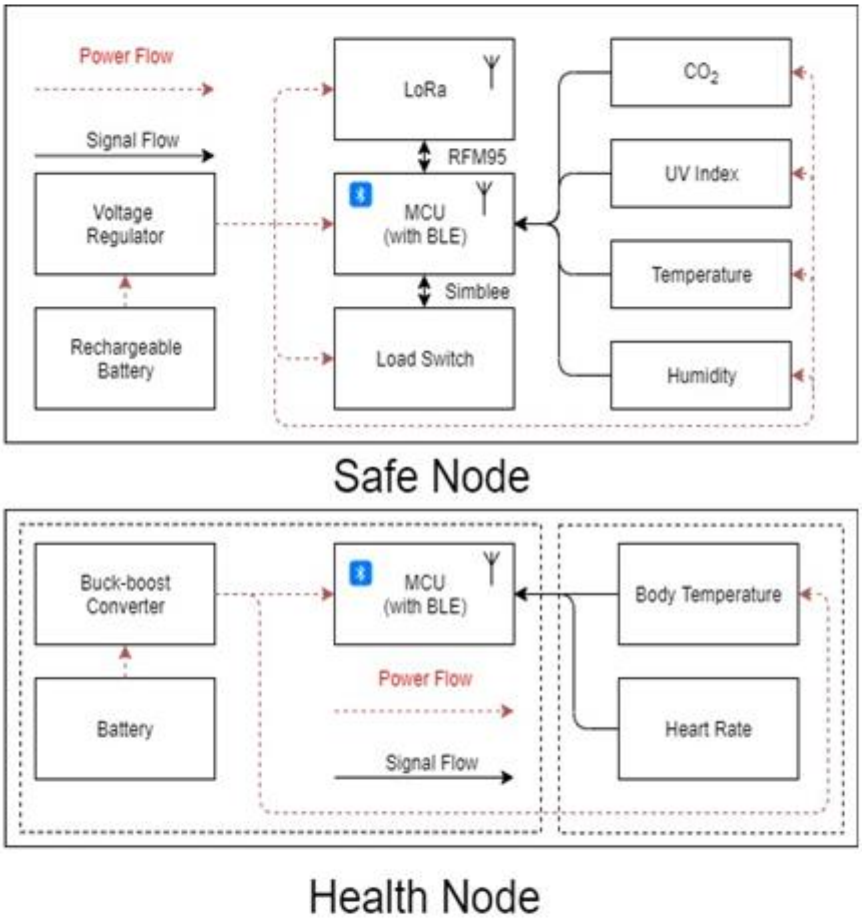


Figure 23. Block Diagram of Safe Node and Health Node

5.2 IoT in Vehicular Networks

5.2.1 Inter-vehicle communication

In inter-vehicle communications, it uses two different type of messages which are naive broadcasting and intelligent broadcasting. The vehicles send naive broadcast messages continual to their neighbor vehicles. The receiver vehicle ignores the message that comes from a vehicle behind it and continues to broadcast the message comes from a vehicle in front to the vehicles behind it. This make sure that all vehicles moving in the same direction receive every broadcast message. The weakness of the naive broadcasting method is that too many broadcast messages that are generated in a short time, cause the increased risk of message collision, and resulting in lower message delivery rates and increased delivery times. Intelligent broadcasting with tacit acknowledgment solves the problems inherent in naive broadcasts by limiting the number of messages delivered for a given emergency event. The supposition is that the vehicle in the back will be responsible for transferring the message along to the rest of the vehicles. Also, if a vehicle receives a message from more than one source, it will respond to the first message only. [148]

5.2.2 Vehicle-to-roadside communication

The vehicle-to-roadside communication represents a single-hop broadcast where the Road-Side Unit sends a broadcast message to all equipped vehicles in the vicinity. The roadside units could be located per kilometer or less, allowing high data rates to be maintained during heavy traffic. For example, the roadside unit will calculate the beginning time and the last time combine with traffic conditions to determine the appropriate speed limit to broadcasting. The Road-Side Unit will regularly broadcast a message about the speed limit and will com- pare with the vehicle data to determine if it needs to apply a speed limit warning to any of the vehicles in the area. If a vehicle is operated over the speed limit, the road-side unit will send a broadcast message to the vehicle to enable auditory or visual warning, requesting that the driver reduce the vehicle’s speed. [148]

5.2.3 Routing-based communication

Routing-based communication is a multi-hop unicast in which a message is transmitted in multi-hop style until the vehicle carrying the desired data is obtained. When a vehicle receives the desired information, the application at that vehicle will immediately send a unicast message holding the information to the vehicle it receives the request, and then it continues forwarding it to the source of request which now is a destination vehicle. [148]

5.3 Behaviors and Decision Making

5.3.1 Smart Buildings

The underlying system and services used in [68] and [54] are very similar since the architecture portion of [68] references the architecture of [54]. [54] states that two different wireless technologies are deployed in the environment it focuses on. [55] refers to an article published in 2012, that discussed the study of IoT implementations for creating ‘smart buildings. This piece outlines the underlying systems for the architecture discussed in [54] when addressing the use of 6LoWPAN. However, WiFi is applicable to only the two portions of the entire architecture that utilize 6LoWPAN technology: The Backbone Wireless Sensor Network and the Gateway interface to the Web. In the Backbone WSN, Constrained Application Protocol (CoAP) is used as a specialized web transfer protocol. It is meant to be used with nodes and networks that are constrained in the IoT. It was created for machine-to-machine applications. According to the CoAP website at coap.technology/impls.html, CoAP is not only used between constrained devices, but also between them and more powerful systems such as cloud servers, central home servers, and smartphones. The rest of the protocol stack for the Backbone is as such: Link Layer uses 802.15.4 standard, Internet Layer uses the IPv6 6LoWPAN protocol, Transport Layer uses the UDP protocol and the Application Layer uses the CoAP protocol. Each of these system protocols were chosen for a specific reason. 802.15.4 offers low power consumption and supports low latency machines. It also utilizes dynamic device addressing and minimal complexity. The protocol offers data rates at 20 kb/s, 40 kb/s, and 250 kb/s according to [54]. In [55], the Contiki operating system is discussed as a part of the actuator services system. The

doi:10.20944/preprints201912.0276.v1

Contiki, according to the documentation available on GitHub at github.com, is an OS for resource-constrained devices in the Internet of Things. The controlling and monitoring of application services system are facilitated by auxiliary services which are provided by control services. These application services are services that specific applications need so they can interact with the system. [55] discusses that in some environments, the physical location of sensors must be known by the system for it to provide information with context. However, modern day location service solutions are not lightweight and would cause more overhead then necessary in the system. To solve this problem, [55] implements a centralized location mapping service which can appropriately assume that the sensors are in fixed positions and people will not be moving them. Maintenance services for the system are quite relevant since smart environments are often time and sometimes safety critical. [55] designed services specifically for this reason by defining a periodic status update service sending sensor readings and node status to a central registry. Also, the individual sensors utilized a service to check for 'heartbeat' of other nodes.

5.4 IoT in Learning Environments

5.4.1 Attendance Systems

Universities can tailor existing technologies to more robustly collect information from students and staff while actively engaged with the campus. Blackboard Learn, an online learning management system (LMS), is used in junction with physical door access control systems to limit entry to specific buildings on campus based on information provided. Information provided from the learning management system can include degree program, gender, and other specific access rights. A magnetic stripe on the identification card can be swiped or pressed against electronic locks to transfer user information from the card to the lock. The smart lock verifies the data against a database with information regarding access rights. The device subsequently activates a mechanical system to unlock the door or provides output that the provided data did not pass the verification. In addition to collecting building access data, universities with existing internet infrastructure can apply the concepts behind IoT to develop a system to collect data more consistent than building access; wireless device location services. Purdue University in West Lafayette, Indiana serves as a prime example. Purdue Air Link 3.0, shortened as PAL 3.0, serves as the campus-wide internet infrastructure for students and staff. The vast amount of wireless access points installed throughout the campus collectively ensure constant internet connectivity. Requiring a Purdue account to connect, PAL 3.0 can seamlessly connect a device to the wide array of access points [109]. With the ability to connect however comes the ability to observe. With access points denoted as sensors in the context of an Internet of Things environment, the university can track account connectivity across the network, providing massive amounts of location and internet traffic data. The university can track where students are connected, and thus cross reference student schedules to detect course attendance and absence. Within an Internet of Things architecture, the diversity of 'things' would exist regarding the sheer variety of devices with wireless connectivity. Data is then 'sensed' or collected by wireless access points. The phenomenon occurs when a device connects to an access point that is broadcasting both 2.4 GHz and 5.0 GHz frequencies. The device uses the signal to interact with the Internet, thus providing the sensor with a wide variety of data. Once collected by the sensor, the data is sent to a repository within the network and analyzed. The variety of "innovative learning" development services the university employs are then utilized to provide meaningful information of the provided data [110].

5.4.2 Distance Education Classroom

In order to better accommodate individuals seeking nontraditional education services, universities have used the Internet of Things paradigm to develop distance learning platforms. Figure 25 clarifies the infrastructure, where the teaching server represents a learning management system [142]. Learners can interact through the virtualized platform with educators and receive personalized teaching based on the tools provided by the learning management system. It should be noted that most distance learning platforms no longer utilize the GPRS methodology for transferring data and do so through internet connectivity. Learners receive personalized exercises from the system and based on input.

Within the context of IoT, this system establishes a connection to online learners that represent 'things' of the system. Each learner emits abstract data in the form of assessments, assignments, and other learning exercises to educators, which represent the sensors of the system. We can define learners and educators as things and sensors, respectively, due to the more abstracted definition of sensing. Things produce information that is then collected by sensors and devices within the network. The data is uploaded to a database module combined with a teaching server. The system's application to IoT is completed with the transfer of data from sensors to the repository for analysis. In this case, the repository is a virtualized database with a learning management system acting as a data analysis factor.

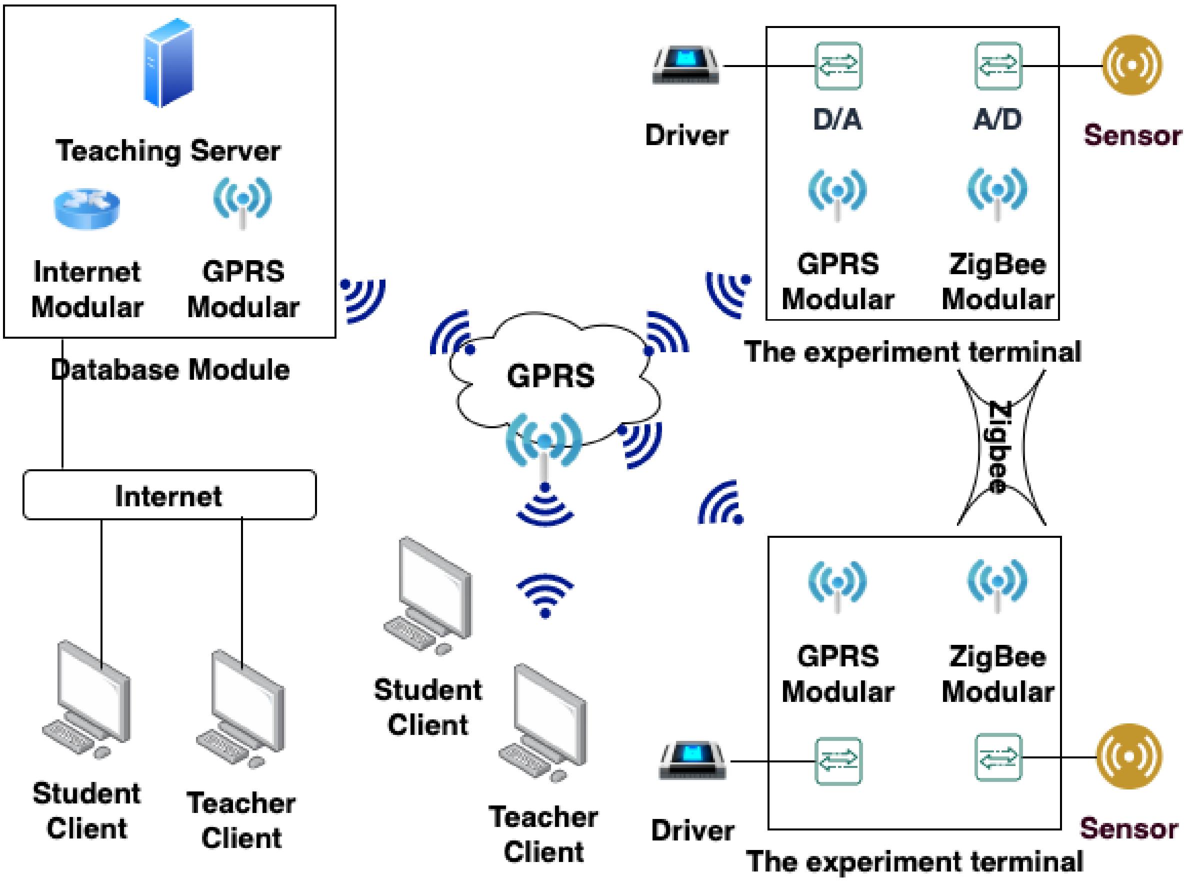


Figure 24. Distance Education System Structure [142]

5.4.3 IoT Learning Management System

An existing Learning Management System implemented an Internet of Things architecture to support better data logging and analytics. Included in the smart devices implemented were RFID lockers, integrated printing services, and other varying student resources like residence air conditioning and local Ethernet connectivity. Figure 26 visualizes the IoT device infrastructure, categorizing aspects per usage. The things of the network are represented by all technological devices visually placed on the edge of the figure.

doi:10.20944/preprints201912.0276.v1

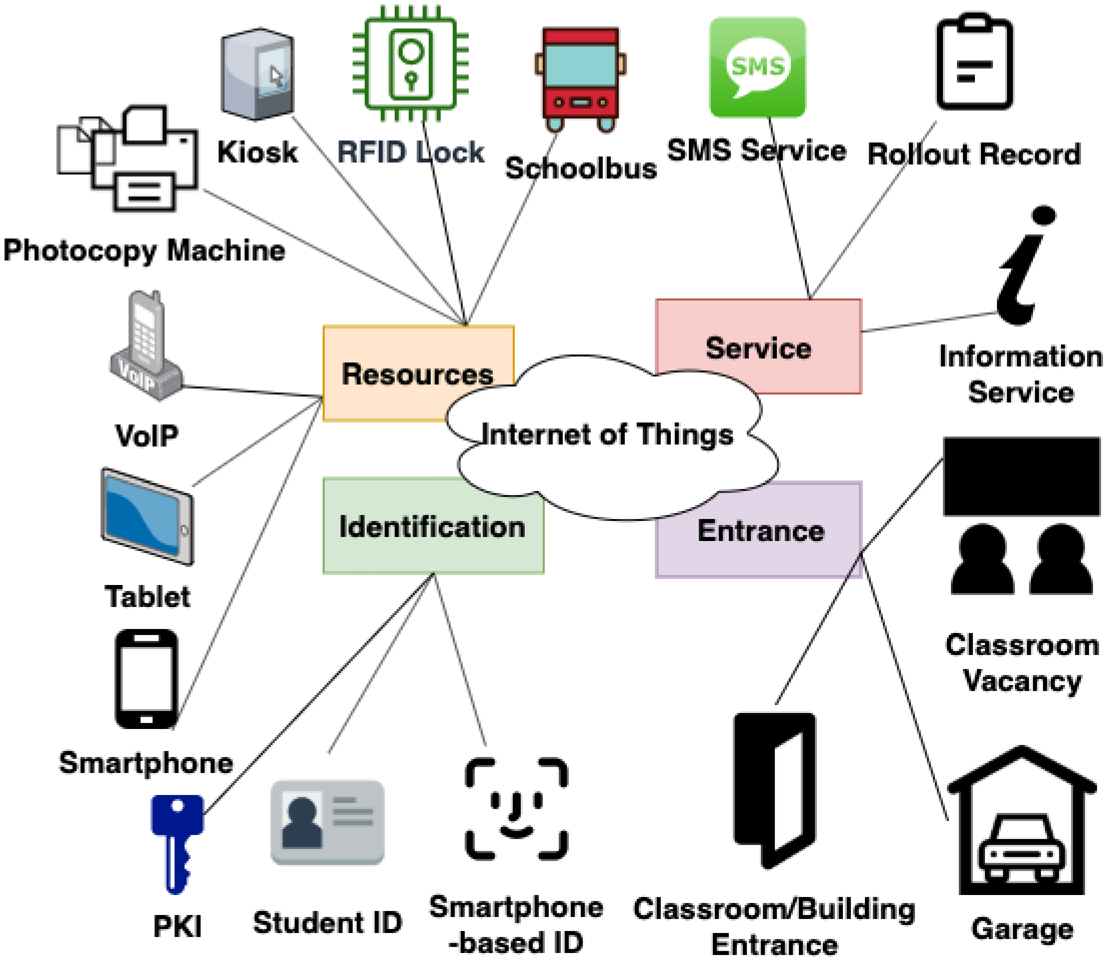


Figure 25. IoT Learning Management System

These include "mobile devices" and "RFID locker". What uniquely identifies this application of IoT is the fact that the things and sensors of the IoT architecture are redistributing data between each other as opposed to transferring data to one source [101].

5.5 IoT in Mining

5.5.1 Underground Cave Systems

Integrating a properly working and stable system within mines is not just a necessary requirement, but also a safety and economic requirement as well. To achieve this in today's world, cloud computing has come to the rescue and is used almost exclusively to handle and manage data. There are four types of data that cloud computing is most used for in mines [34]. (1) Multisource High Heterogeneity Data, (2) Huge Scale dynamic Data, (3) Low-Level with Weak Semantics Data and (4) Inaccuracy Data. When it comes to technology, there are many types of data and countless ways to interpret that data. The problem resides with how a computer or system should interpret received data into understandable information that is correct and accurate. To solve this, these data structures were made to help sort data into its proper area. Multisource High Heterogeneity Data consists of varying characters and integers to form information in the form of media. This ranges from cameras, photos, video streams, audio communication, and EM waves. This type of data supplies miners with most of the surveillance and communication technologies and helps establish a system of working parts. The world of information technology and data transfer is extremely large and is only growing by the year. While transmitting data from point to point may very well be relatively simple, having a consistent stream of large amounts of data running at all times of the day is another story as traditional technology often become interrupted or lose data when constantly transferring large chunks. Huge scale dynamic data comes into play to help solve this issue. This works by connecting many sensors together in a mesh like network to create numerous paths that data can pass through. Using this type of network, data being passed from one node to another in a consistent manner can be achieved by finding the shortest and most connective path possible in the network. While sensors are a cornerstone to mapping out the safety and complexity of a mine, they provide low amounts of data at a time which alone is useless to an industry. This introduces the area of Low-Level and Weak Semantic Data. This area of data helps build deep and complex semantics from many chunks of low-level data to create enough information that can be easily interpreted by engineers. It has been proven that oftentimes, especially in cave systems, that initial data that has been received from sensors is partially incorrect or malformed. This is again due to the data being reflected or refracted when passing through hard-to-pass objects such as rock and heavy metals, resulting in an average of around 30% percent of all received information being correct. This area of data is called Inaccuracy Data and helps to detect flaws in received sensor packets by using a method called multidimensional data analysis to process what can be verified as being true, and what needs additional testing to prove the sensor data to be true.

5.6 IoT in Energy Systems

5.6.1 Smart Grid

Smart grids are already a big part of our life. They allow companies to monitor usage using 2-way communication. Our current electric grid was conceived more than a century ago [52]. This grid was designed based on rudimentary electricity needs. People during this time only needed to power a few lightbulbs, radios and basic electrical devices. Electricity demand now is much more intense and random compared to the first grid implementation. Smart energy grids upgrade the current grid system by using 2-way communication [52]. Instead of the factory producing energy and sending it into the grid at set times, houses can request electricity and factories can accommodate to match this instantaneously. A 2-way dialogue is introduced by the smart grid. Now a smart meter can transmit data to the electricity company and request electricity. This is a game-changer for grid demand and allows companies to anticipate, collect data and respond to grid demand more efficiently and quickly [52]. This in turn reduces the environmental impact and allows companies to waste fewer resources and homeowners to save more money. Smart devices can be added to a (HAN) home area network and controlled to run at certain times. By communicating with the energy grid, these devices can be set to run during times of low demand. This reduces the cost of electricity for homeowners and takes some demand off the grid at busy times. Renewable energy solutions are often directly influenced by weather and are unreliable at times. By using communication on a smart grid, these devices can be set to run at optimum times so that the grid is not overloaded or shortchanged [52]. When electricity can be deferred away from peak usage times during the day, customers can expect less expensive bills because less efficient backup facilities do not need to be used [52]. Most of the concerns about smart grids come from privacy and RF radiation risks. The grid itself seems to be a good idea in concept and its pros are extremely prevalent against its cons. RF has been a large concern of the general public and many people are not comfortable with not having safety measures in place to regulate our exposure to it. Many people believe that current RF acceptable exposures are unsafe. Adding multiple smart devices into your home to help regulate the smart grid will add numerous points of RF radiation. Devices include dishwashers, microwaves, stoves, washing machines, dryers, air conditioners, furnaces, refrigerators, freezers, coffee makers, TVs, computers, printers and fax machines to name a few [85]. These appliances will operate between 917MHz and 3.65 GHz several times per minute. Smart meters will also be transmitting outside so this radiation will be prevalent everywhere [85]. The other issue is privacy. Storing your data with electricity companies means that your data is only as secure as the company guarding it. If hackers are able to obtain your data, they could determine how much energy you are using, how many people are living in your home, what times you use utilities, and what times you leave without ever looking at your home. The smart grid consists of millions of moving pieces and parts, controls, computers, power lines, new technologies and equipment [52]. Every day new pieces are added, and different technologies are brought online

doi:10.20944/preprints201912.0276.v1

to further improve the grid. The grid will continue to evolve into the future as new technologies are created to improve it. Many people are against smart devices and grids because of privacy concerns and RF wave exposure. Some legislature has arisen as a result of unhappy customers and the smart grid has faced backlash in some areas. Regardless, the smart grid is currently in full swing and continues to grow and evolve as it will into the future.

5.6.2 Zero-Energy Buildings

Zero-energy buildings are a new form of technology that utilize a smart grid to communicate and distribute energy efficiently. They use a variety of IoT technology and new sensing techniques to generate renewable energy and power themselves. Some of these buildings have on-site energy storage which helps reduce demand for the grid and further increases their efficiency. They can be summarized as a building that has a net energy consumption of zero [8]. This means that these types of buildings use various energy-efficient and saving techniques to achieve a net value of zero energy consumed and some can have a negative amount of energy consumed due to their ability to contribute energy to the grid. Zero-energy buildings can achieve net-zero energy consumption by different techniques. Most buildings will be connected normally to an energy grid and use power from the grid as necessary. Most zero-energy buildings have some form of renewable energy to create energy for themselves. These buildings will utilize their self-created energy when available as many renewable forms of energy such as wind and solar power and heavily dependent on the weather. When weather conditions are good, the building will create its own energy and not rely on the grid. If the building has perfect conditions or low usage, it may create an excess amount of energy. Smart grid technology allows the building to distribute energy back into the grid and contribute to offset the times it needed to pull energy from the grid [4]. This offset is measured and used to calculate the building’s efficiency. If the building can support itself over the course of a year and make up for any energy it took from the grid, it is considered a zero-energy building. Zero-energy buildings can be combined into zero-energy towns to multiply this effect and further reduce environmental impact [4]. Below is an example of a zero-net energy building that could be used today. As shown in the figure 39, a zero-energy building usually has multiple forms of renewable energy to power itself and contribute back into the grid. This Figure is an example of what a typical house could look like. An office could use similar technology to achieve the same goals. This house features several energy-saving designs. Energy optimized windows typically involve a window using double pane vacuum-sealed glass. The vacuum acts as a good insulator and lets minimal thermal exchange occur between the air outside and the air inside the house. A geothermal heat pump uses the constant temperature underground to pump in heat or cool air when needed. This helps reduce the load of a conventional heating system and allows the ground to cool or heat the house instead of using electricity. Another good optimization is the use of solar panels in conjunction with a wind turbine. This creates two forms of power for the house alongside the backup smart grid. These renewable energy tactics allow

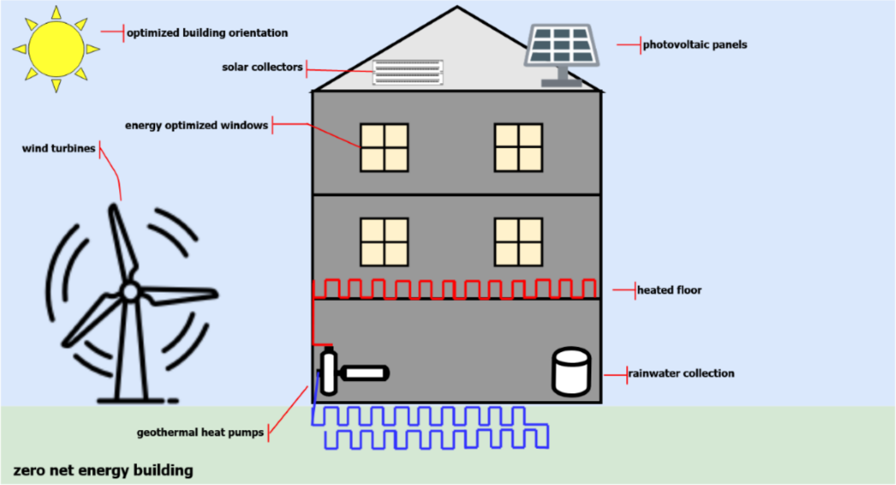


Figure 26. Zero Energy Building

the house to be even more enough during different weather conditions so the owner can reduce their environmental footprint further. The orientation of the building is also important. The building needs to be oriented so that natural sunlight can heat the house when needed. A few other additions include heated floors and high-quality insulation. The heated floors allow for better conservation of energy as the conditioning system is not working against the temperature of the floor. Efficient insulation is used here at a higher cost, but ultimately a payoff in the long run when this house can produce electricity for itself and become a true zero-energy building. Typically, a zero-energy building costs 10% more on average to build than a traditional energy-hungry home [4]. This ends up paying for itself quickly because typical zero-energy homes save around $125-$200 a month which adds quickly to pay for the construction cost expenditure lost in buying more expensive materials and complicating installation processes [4]. Most of these buildings get half or more of their energy from the grid [8]. Unfortunately, this means that a large amount of power is still being drawn from the grid and these buildings are not self-sufficient all the time. The offset to this is that the buildings contribute this energy back into the grid when weather conditions permit. A problem with the zero-energy home is that it can be a lot harder to find a contractor with the ability or willingness to build it [8]. Another issue that can arise is that with more companies producing renewable technologies, prices continue to drop on renewable energy equipment [8]. If you build your home today, the equipment you may use to install may be obsolete in 10 years and worth a lot less. This will decrease the value of your home and may make it difficult to sell it for what you put into it. Although these buildings typically have a larger construction cost, they pay for themselves quickly and provide measurable environmental carbon reductions. Hopefully, we will see more of these buildings implemented as renewable energy technology develops.

5.7 IoT in Energy Systems

5.7.1 Smart Parking

All IoT parking systems will require some combination of sensors and transmission methods to function. However, there are differences in how drivers are routed to parking locations and how they can be scaled. Some of the proposed systems include: parking guidance and information system (PGIS), transit-based information system (TBIS), centralized assisted parking search (CAPS), opportunistically assisted parking search (OAPS), non-assisted parking search (NAPS), car park occupancy information system (COINS), parking reservation system, agent based guiding system (ABGS), and automated parking [15]. The differences between system functionality and processing is listed as follows:

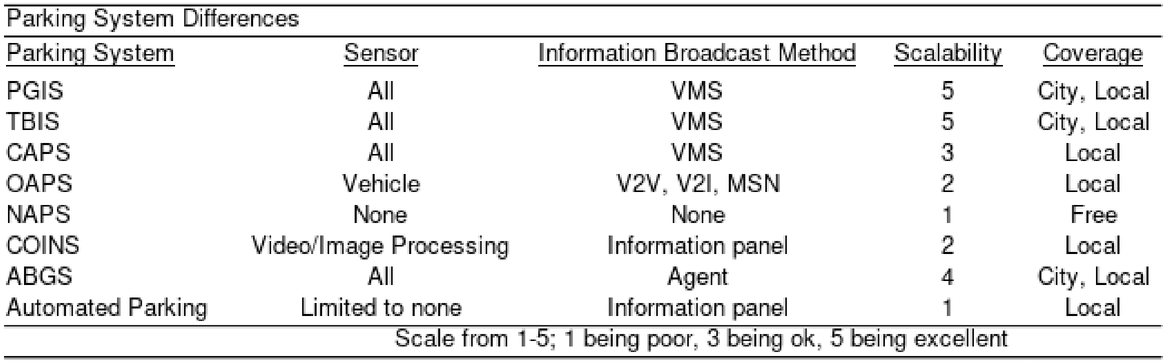
- **PGIS** uses various sensors to collect data which is then sent to drivers to notify them of vacancies [15]. There are many adaptations of PGIS that use various other technologies to solve other more nuanced issues like using additional sensors to improve system reliability.
- **TBIS** prioritize the use of public transit systems instead of simply advertising empty parking spots for private vehicle drivers [115]. Transit use is encouraged by monitoring and allowing reservations for convenient parking spots near transit stations. By allowing commuters to check and reserve parking spots near mass transit stations, it encourages people to park their vehicles at the station and use mass transit instead for the day.
- **CAPS** use vehicle and parking lot sensors to detect open parking spots, but has all information be passed on to and processed by a centralized server responsible for maintaining an up to date status of the parking garage [81]. Drivers seeking a parking spot will query this central database and be directed to a guaranteed spot.
- **OAPS** has each vehicle equipped with a wireless communicator and sensors enabling them to detect open parking spaces and share this information with other vehicles essentially forming an ad hoc network [81]. Unlike CAPS, this system has no single server which receives all updates and maintains an up-to-date status log. As such, cached parking information on each vehicle may be outdated or inaccurate and drivers must be aware of the possible inaccuracies.
- **NAPS** is when no smart systems are employed at all

• **COINS** is a parking management system that is dependent on only a single sensor. This sensor is usually a video or image recording device that takes a fixed image of the parking lot. The image is then processed using various image recognition algorithms to identify empty parking spots which can then be displayed to drivers [29].

• **ABGS** is not so much a smart parking system as it is a tool for research, urban planning and development. Sustapark is an agent-based model for simulating parking behaviors. It does this by defining drivers with different interests, and simulating parking locations and city traffic [127]. The resulting simulations can then be used by city planners to design proper parking spots and roads to help ease road congestion.

• **Automated Parking** are systems where drivers do not search for parking, but rather leave their locked vehicles in a vehicle bay area. An automated system will then move the vehicle to a designated parking spot. Retrieving the vehicle can be done using a password or any other form of authentication system that can be implemented based on need [74].

Figure 27 is adapted from Al-Turjman, Malekloo [15] which compares the different parking system types in terms of features and important value metrics.



Parking System Differences

Parking System	Sensor	Information Broadcast Method	Scalability	Coverage
PGIS	All	VMS	5	City, Local
TBIS	All	VMS	5	City, Local
CAPS	All	VMS	3	Local
OAPS	Vehicle	V2V, V2I, MSN	2	Local
NAPS	None	None	1	Free
COINS	Video/Image Processing	Information panel	2	Local
ABGS	All	Agent	4	City, Local
Automated Parking	Limited to none	Information panel	1	Local

Scale from 1-5; 1 being poor, 3 being ok, 5 being excellent

Figure 27. Characteristics of various smart parking systems [15]

From the figure, the various implementations of car parking systems that could be used in a smart city have a variety of costs and benefits. The sheer amount of proposed systems is a sign of academic belief that smart city technology is a field with many research opportunities. In term of the overall state of IoT in smart cities, this research in parking systems indicates potential challenges as well in the form of standardization.

5. Challenges

Advances in IoT technologies is transforming healthcare with the introduction of several new applications and services. However, 74 percent of these IoT initiatives are unsuccessful [94], as the new technologies bring new challenges. As the medical devices are directly connected to the patients the performance of these devices is very vital leading to tighter functional and technical requirements. Any problem with device can cause a serious impact on the patient and hence it is very important to understand the sensitivity of this and work towards the betterment of the performance. Current limitations include energy and mobility limitations, memory and computational limitations, security limitations, regulatory challenges, environmental challenges, vendor challenges, data handling challenges, etc. Some of these challenges are explained in more detail below.

Security challenges: Security requirements are the key challenge IoT need to address as the healthcare data requires highest confidentiality and reliability. Conventional methods of security do not provide the needed solutions encountered in the fast-paced development in the IoT in healthcare [122]. It was found a recent ZingBox study which was done to understand IoT software and it revealed that hackers can gain access to the confidential information by simply looking into network traffic for error messages [33].

Computational Limitations: Most IoT devices have low end CPUs with low speed processors. As the perception layer devices are primarily designed as sensors, they lack the necessary computational capacities. Currently to overcome this limitation the computational aspects are dealt in other layers. With miniaturization of processors future sensors will have adequate processing capabilities [49].

Memory Limitations: Just like the processor speeds, these devices do not have enough memory space. To overcome the low memory IoT devices use embedded operating system, system software and application binary, however, memory limitations make the device manufacturers to sacrifice security protocols leading to security threats. New middleware solutions to address security weakness are being implemented [67].

Energy Limitations: IoT healthcare uses devices like body temperature and BP sensors which are low power devices which can switch between active and power-saving mode reducing the energy consumption. With advances in charging through Wi-Fi or Bluetooth radio waves will make battery-free IoT sensors [102]. Wearable sensor node with solar energy harvesting are also being developed to reduce battery capacity requirement [140].

Dynamic Topology for Mobility: By nature, healthcare devices are usually mobile such as wearable body temperature sensor or heart rate monitor which are connected through wireless networks to cloud. With more emphasis on "Anywhere, anytime" more and more health care services are added to the IoT Platform make give patients more refined experience [13].

Scalability: With exponential growth of number of IoT devices connected to the network and as more and more services are added to the IoT application platforms, solutions developed are not able to keep pace with the system requirements. It is very important to develop the right architecture/framework and systems which can provide the scalability to handle the anticipated growth [100].

Communication Media: Healthcare devices use multiple types of wireless communication methods like Zigbee, Z-wave, Bluetooth, Wi-Fi, 3G/4G, etc. However, these wireless networks do not provide the necessary security protocols the conventional wired networks provide more so in case of IoT due to the large number of devices being added and the mobile nature of these sensors. New protocols need to be developed to prevent data losses due to network congestion, provide security and reliability.

Multiplicity of Devices and Protocol Networks: The IoT network has multiple devices ranging from the simplest devices like the PC to more complex devices like low-end RFID tags. The devices vary based on processing, memory, computational powers and network connectivity protocols. It is a challenge to create a protocol standard which can deal with the plethora of devices and networks [64].

Government Regulations Challenges: As IoT continues to gain popularity more and more sectors started adopting this new technology to develop and deliver more products and services. The data/information collected and transmitted by these devices over the network has become more critical and confidential, making cyber security an utmost important necessity. To address these issues the US government had passed a bill "The IoT Consumer TIPS Act of 2017" and "The SMART IoT Act" [47]. The Act is followed up by "The Internet of Things (IoT) Cybersecurity Improvement Act of 2019" which was introduced by the United States Congress on March 11, 2019.

It is expected that the UK and other countries will follow by introducing similar legislation. However, by nature IoT like internet it is difficult to be regulated by any single Act or Policy by any government as technology connects across multiple regions/countries making it difficult to implement effectively such policies. The industry and the community should try to self-regulate so that the technology is not exploited for the wrong reasons.

Environmental Challenges: As more and more devices are being added to the network and the energy consumption of the devices is increasing rapidly. This means that better green technologies need to be implemented in order to make the system a lot more energy efficient and less electronic waste generation.

IoT Vendor Challenges: IoT technologies provide tremendous opportunity to provide best possible healthcare solutions for patients and reduce the overall cost of healthcare. Several vendors jumped into provide their own custom-made applications which are not tested. As there is a lack of Industrial Standard for products are services, selection of the right vendor has become challenging. Healthcare being a very sensitive area with far fetching implications vendor/product validation like other medical equipment need to be adopted. However, coming up with agencies which can certify reliable, secure, scalable, and efficient product or service provider is going to be challenging [76].

Data Handling Challenge: IoT services in healthcare are just at the beginning stages and already it has started to generate large quantum of data leading to serious data handling challenges. With the addition of several new applications and several more devices the data handling problems is going to be a major bottleneck for IoT to penetrate further. New technologies are being developed for better storage and faster data analytic solutions; however, it has been seen if they can catch-up with the IoT device and data explosion [107].

The full implementation of IoV system will change drivers' experiences completely with integrated smart sensors and devices. These hardware serves to be functional in the same way as different sensing parts on human body and further improve sensitivity to internal and external environment. Except for driving experience, IoV system can significantly enhance the efficiency in traffic management and safety and reduce timing in logistics and transportation. However, all benefits cost increasing financial investment in infrastructure construction and maintenance, vehicle production and car insurance. On top of the cost, the implementation of physical and communication layers becomes the most challenging parts in the realization of IoV. Some of challenges are described as follows:

Localization challenge: Localizing vehicles accurately becomes tremendously significant and challenging since the requirement of detecting relative distances between immobile and mobile vehicles in a modern city has exceeded localizing accuracy of GPS-based localization technique [11]. Moreover, GPS signals can be easily blocked in a highly populated city. To meet the accuracy requirement, the following issues are recommended to address:

•The accuracy of tracking and localization is suggested to be 50 cm while the current GPS technology only support the accuracy of 5 m (ibid.).

•GPS localization detects longitude and latitude at a certain frequency but do not feedback any speed parameter, which is expected being regulated globally in vehicular communication environments [144].

•Because of highly populated buildings in a modern city, the deteriorated GPS signal becomes main constrains, limiting tracking and localization efficiency and effectiveness [59].

Location privacy: To fully monitor and control self-driving vehicles in the highly mobile ad hoc-based network environment. Periodic information, regarding to speed, lo- cation, acceleration and other types, are necessary [62]. However, the shared location information might bring up privacy concerns. Consequently, the IoV system must acquire necessary information without causing any unwanted information leakage. Therefore, keeping the location information safe becomes one of potential challenging research works [44]. There are some suggested techniques, such as pseudonym [72], silent period [133] and mix zone [146], to tackle this privacy concern. However, none of these techniques could solve the privacy concerns completely because of the following reasons. The pseudonym is effective only if the vehicle density is high. This technique loses its privacy effectiveness at low vehicle density. Silent period is not applicable to real- time location monitoring and mix zone technique maintains its usefulness on multi lane scenario but not on one lane scenario.

Radio propagation modeling: Radio propagation is expected to be accurately modeled so that vehicles' response time to emergency can be predicted and optimized. Highly populated infrastructures in a modern city deteriorate the signal strength greatly due to high reflectance coefficient along the signal propagation path. The moving radio obstacles contains trucks, buses and mini vans while the static obstacles include buildings, tunnels, and bridges [111]. The modeling of radio propagation becomes challenging as the WAVE standard demonstrates lesser penetration capability than Wi-Fi and other RF-based techniques due to high carrier frequency of 5.9 GHz. The modeling task could be finished if the following research questions can be answered:

•The radio propagation model is expected to contain the impacts from both moving and static obstacles [125].

•The model should accurate to predict signal strength in line-of-sight scenario even if communication takes place with the low penetration capability.

Other challenges: To fully achieve a mature IoV system, enormous data received from different types of network should be processed and computed effectively and appropriately. Operational data management and processing becomes one of unique important task. Apart from data management, other challenging works, related to MAC standard [87], opportunistic framework [35] and geographic routing [78], have been brought up for more efficient solutions.

The use of wireless IoT in the field of monitoring behaviors and decision making has shown a great deal of success with multiple implementations, but there are also many challenges that these technologies face.

New Technology Challenges: Many of the technologies used for this purpose are relatively new and sometimes aren't fully developed. This presents a challenge, because this type of technology is so new, it will have more issues than technology that has gone through many iterations and will be more expensive to support.

Cost: This leads into the next challenge that these kinds of technologies face and that is the cost. While there are low cost solutions to monitoring behaviors and decision making such as the method shown in the research paper "Smart Behavioral Analytics over a Low-Cost IoT Wi-Fi Tracking Real Deployment," many of the solutions are very expensive to implement. An additional factor in cost that must be considered is the cost of the backend servers to process the data that the sensors pull. This of course depends on the type and amount of data collected by the sensors as well as the number of sensors that are collecting data. Software costs must also be considered for the servers as well as the sensors themselves if applicable. If an in-house software is going to be developed and used, the time needed to develop, and bug test the software can be a substantial problem.

Security: As discussed in the paper "Smart Behavioral Analytics over a Low-Cost IoT Wi-Fi Tracking Real Deployment, [17]" one problem several wireless IoT solutions came across is the fact that people can spoof or change their MAC addresses on their wireless or wired devices. This can prevent more advanced tracking systems from keeping track of and identifying the locations of individuals. Furthermore, MAC addresses can be spoofed to allow someone to impersonate another person or their device. This ability for people to change their MAC addresses can make it difficult for these systems to accurately track individuals. There are a few solutions to this problem, one is to rely on the number of MAC addresses rather than the value of the MAC address itself. This is the approach that the researchers in the "Smart Behavioral Analytics over a Low-Cost IoT Wi-Fi Tracking Real Deployment" [17] paper had gone with. This approach allows for the system to gather information about the density of people in an area without being able to identify, to any meaningful degree, an individual. This approach limits the usefulness of a behavior and decision monitoring system as it's difficult to detect the choices of an individual. For example, say a shopping mall implemented a behavior and decision tracking system to see which store people favored. The system could be used to count the number of people at any moment and analyze trends such as the times of the day that a store is the most popular. This kind of system couldn't isolate an individual and track them across the mall to see what other stores they favor. This limitation makes it difficult for systems such as these to be more than just population counters.

Interference and Attenuation: Another limitation or challenge that wireless tracking systems encounter is caused by the nature of electromagnetic waves. Electromagnetic waves are highly susceptible to interference due to the large number of wireless devices that people use. Phone both connect to local wireless area network as well as cell towers. Other things such as lights and electric motors also can introduce interference to electromagnetic waves. Other things such as wall material and density can have a great effect on the propagation of a wireless signal. Even people can absorb electromagnetic wave and decrease their propagation. Another source of interference is other sensors within the system communicating with one another or a central hub. All these factors are things that need to be considered in order to successfully implement a wireless IoT system. These kinds of systems may also face issues with a changing environment such as an auditorium. When the auditorium is empty or has very few people sitting in it, the signal propagates differently than if it were filled. These changes when not accounted for in the design and placement of the sensors could render them useless or ineffective in certain situations.

Flash Effect: Another example of a more specific issue that a group of researchers in the paper "See Through Walls with Wi-Fi" [56] came across when doing research with using radio frequency waves to detect people within an area was the flash effect. As explained previously, the flash effect is caused when the RF waves reflect off the walls of a room and are picked up by the receiver. As stated in the paper "See Through Walls with Wi-Fi," [56] these signals are stronger than the signal that travels through the wall, reflects off the object being tracked, and back through the wall again. The sensors then have trouble differentiating between the signal of the person being tracked and the reflected signal. Using a multiple input multiple output transmitter and receiver would help to lessen this issue by causing destructive interference of the reflected wave but, these kinds of radios are more expensive to purchase than one that does not implement the MIMO technology.

Multiple Data Sources: Another problem that is particularly encountered in using wireless cameras to monitor behavior and decision making is the extrapolation of multiple data sources to create usable information. These wireless camera systems require a great deal of backend processing in order to get usable information. In addition to this, they need to send a lot of data back through the network to send to the server that processes the images taken. These systems may have some difficulty sending the information back depending on what wireless technology they use. It's also worth noting that these systems are extremely expensive to implement and maintain.

Every technology has its own set of challenges that need to be overcome in order to proceed in creating something useful. Wireless IoT used for monitoring behaviors and decision making is no different. These challenges ultimately result in new innovations that can not only be implemented in the case in which it was designed for but, to improve wireless technology as a whole. Furthermore, as wireless technology improves, so will the research in this field.

Opt In/Out of System: In many learning environments, the implemented Internet of Things networks are based on devices that students previously own or are required to own. If an IoT system is developed in such a way that requires students to acquire additional technologies, there may be a significant decrease in participants due to disinterest or lack of availability.

Security and Privacy Concerns: With each layer of added technical capability comes the need for increased security built into a system. With an Internet of Things network each device requires more advanced security mechanisms to safeguard communications across the network. As sensors within an IoT environment are traditionally low power, this restricts the variety of processing devices used. Due to that

System Size Restrictions: Devices connected to an IoT infrastructure must remain in communicative range with other components of the system while still optimizing the system's area of effect. Each learning environment will require a personally designed IoT infrastructure to optimize device effectiveness.

Proxied RFID Attendance: Implementations of an IoT infrastructure to track student attendance cannot account for students who bring multiple RFID tags as a means of falsifying a fellow student's attendance on their behalf.

Dedicated Internet Infrastructure: Most real time implementations require centralized, dedicated network servers to support the resource needs of receiving, processing, and storing Internet of Things device data. Absent of proper resources or funding to obtain similar resources, an implementation of IoT may not be successful. Wireless communication, as discussed, is a foundational component to an IoT architecture. This suggests that systems absent of this component may not qualify as an IoT system.

Terminology Restricting Search: Throughout the literature review process, it was noted that many researchers refrain from explicitly defining the characteristics of an Internet of Things system as a whole. This is to say that what qualifies as an Internet of Things system lacks clear distinction. Due to this, there exist systems that are architected and implemented with a framework like those that are categorized as an IoT system but lack recognition or documentation within the respective research.

Hostile environments and poor network infrastructure may result in inefficient communication. The communication network is not just a one-time setup, it needs to be maintained especially after every drill, disasters, explosions, fires, roof-falls, emergency etc. Some of the factors which affect UMC are:

1. Extreme Path Loss

2. Reflection/Refraction
3. Multipath Fading
4. Propagation Velocity
5. Waveguide Effect
6. Noise

Multipath Fading: One of the largest challenges of communications in mines occurs with multipath fading. This occurs when data is transmitted in different or alternative paths which causes degradation in the strength of the wavelength as well as changes in phases. This especially tends to happen in areas such as in caves or near mountains where various minerals, metals, and rocks can greatly interfere with the transmission often weakening its range or simply blocking transmission altogether.

Reflection/Refraction: Reflection and refraction problems also play a similar role in the area of transmission. When WUSN devices are deployed, they can link up and communicate with both underground and surface devices. The issue with this is that at times when an electromagnetic wave reaches the ground/air interface, it can be partly reflected into the ground as well as part of it being refracted back into the air. Often this can cause incorrect readings of data and false information to be received.

Software Challenges: Various software defined challenges also exist with UMC devices. While systems can be upgraded in the future to provide a 5G LTE private network, it is not necessarily true that these devices are likely to handle the upgrade. The reason 5G can offer much better speeds than its counterparts are because it is utilizing a much smaller wavelength. While this does improve the transmission of data, the range or distance that this can be integrated with is significantly decreased due to the shorter wavelengths.

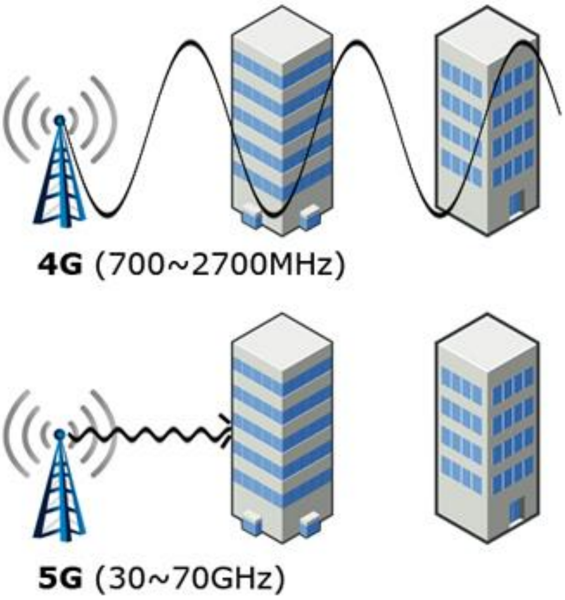


Figure 28. 4G vs. 5G wavelength capabilities

Propagation Velocity: These wavelengths also are much weaker than its predecessors as these radio signals have trouble passing through various materials such as walls, buildings, cars, and it is even reported that rain and storms can block these waves as well [149]. If wide networks are being deployed in cave systems and an upgrade to 5G is performed, various issues such as sudden disconnected devices and communication interruptions can occur. Figure 8 depicted below illustrates such issues with an upgrade happening.

To summarize the challenges, authors in this report draw a table from research done in [50]. These are inherent challenges in a typical underground coal mine.

1. Electromagnetic Interference (EMI)
   - Running of mining machinery
   - No proper electrical ground system

- Bad shielding of electrical items

2. Reduced Propagation Velocity
   - Presence of dielectric materials such as rock and soil
3. Signal attenuation
   - Number of turnings and corners
   - The presence of stopping for direction of airflow
   - Blocks by mining machineries or by roof-fall supports
   - Absorption, scattering, and bending losses
4. Multipath Fading
   - Waves are sometimes partially transmitted and partially reflected
   - Channel capacity and outage behavior
5. Noise
   - Running of mining machinery
   - Drilling, blasting, and conveyor belt system
   - Presence of power lines and electric motors, etc.

By now, it's a well-known fact that mines don't have an even structure. Therefore, authors in [113] identifies crucial characteristics which hampers the communication and connectivity. These are important to identify before researching and starting an experimental setup in such dense and deep areas.

1. Structure
   - Unevenness and roughness of the walls/ceilings cause drastic attenuation of the radio signal
2. Limited LOS
   - Arises due to support infrastructure (of different shapes and sizes)
3. Waveguide effect
   - Becomes operational at certain frequencies
4. Ionized Air
   - Has effect on signal attenuation levels
5. Heat and Humidity
   - Significant increase is experienced with greater depth, and affects propagation and characteristics
6. Noise
   - Signal detection is a challenge
7. Hazardous Gas
   - Presence of gases CH_4, $CO_{2,}$ SO_2, H_2S

As with any new systems being implemented in technology, there are always challenges that slow down adoption of the technology and IoT in energy systems face challenges just other technologies [37].

Integration: One of the main challenges that companies face when trying to implement IoT solutions into their network is that they have problems trying to integrate the new system with the system that is currently in place that must keep running [37]. When implementing a new system, one thing that utilities can struggle with is lacking the proper skillset, which is hard to find in the energy sector [37]. This causes projects to get dropped quickly. In order for utilities to take full advantage of IoT in the energy grid, they are required to buy all in and hire proper teams to implement and oversee the project. Following the project, proper staff should be hired to maintain the infrastructure [37].

Security: With all these new IoT products being added to the energy grid, there is a lot more data that is being generated [37]. One of the biggest problems that utilities face is security over all this new data they get [37]. Most of the data is critical consumer data, which if in the wrong hands, could be disastrous not only to the utility, but also the consumer [37]. Most utility companies' data policies are not suited for this amount and type of data, which forces them to revisit their data policy when implementing IoT systems [37]. Since there is a larger amount of confidential data than a utility is typically used to, it can incur large costs to keep the data safe from cybercriminals [37]. Since there are a lot of costs associated with protecting the data, it sometimes deters companies from pursuing converting their infrastructure to IoT [37].

Power Consumption of Sensors: In IoT systems, there are many sensors to track data and creating those sensors can be one of the biggest challenges in the IoT ecosystem. The hardest part about designing these sensors is creating an energy-efficient, low-power sensor with a battery that can last the lifetime of the sensor [27]. There are a few different ways that sensors can help reduce the power usage of the sensor. The more accurate the sensors are, the more power they consume [27]. To help solve this, there can be an array of lower accuracy devices to create a cluster with a higher accuracy of data [27]. Currently, if a utility wants to use video to monitor the grid, it requires a large amount of power to encode video to upload. In order to reduce power usage, new algorithms must be formed to make the encoding more efficient [27]. Traditionally, analog circuits require a lot more power, so it is recommended that digital circuits are used to reduce power consumption. The need for accurate data is required, but it is not the only thing needed as historical data is also required to get the most accurate predictions for real-time operations [27].

Connectivity: Getting all these devices connected to the internet is one of the biggest challenges that utilities experience when trying to implement IoT [27]. Finding the right technology to do all the connectivity is not realistic. The challenge is finding the best way to get the different technologies to work together seamlessly [27]. Typically, in-home automation, Bluetooth and Zigbee are used to connect the devices to Wi-Fi and then routers send the data to the internet [27]. An ideal solution would be to build a device that would have all the protocols to connect to the internet in one device. The problem with trying to get all the protocols into one device is that most of them use the same 2.4 GHz band and interfere with each other when close to each other [27]. To get devices that use 2.4 GHz to work together, the device must understand the application and the traffic that is being sent. Data to and from the cloud is sent via Wi-Fi, and when sensor data is trying to be received or sent, it uses ZigBee from the gateway, and the gateway uses Wi-Fi as an access point so diagnostics and configurations can be done [27]. Currently, there is research being done to help secure the data being sent over these devices.

Batteries: There are many ways for power collection on these devices, such as RF, solar, sound, vibration, and heat, depending on where the device is and what functions the device performs [27]. The challenge with incorporating power management into the devices is that most of these devices require a battery or harvest their own energy [27]. Since these devices sometimes must communicate, far mesh networks are used to lower power usage since it only must transmit to the closest device instead of the gateway [27]. All these different methods help reduce power consumption, which improves power management.

Privacy: The toughest challenge in IoT in energy systems is the privacy and security required since a cyber-attack could lead to loss of lives, or a massive blackout, which could cause issues across the nation [27]. There have already been instances where IoT enabled medical devices, cars, and smart grid infrastructure have had attacks reported [27]. Not only do each of these devices have to be secure by themselves, but it is also required that the devices are secured in one ecosystem that operates seamlessly [27]. The ecosystem can use a layer model to help secure it, where all the data is encrypted. It is required that there is physical and network security [27]. Users should have security awareness training to help them realize how to keep the devices they are working on secure and use logging and reporting to find out what users are doing [27]. Firewalls, intrusion detection, and prevention systems can be used to help detect attacks that have security policies and processes set [27].

Wireless Medium: Cellular and wireless mesh are two different ways to send data to the cloud for IoT devices, but both have challenges with them. For cellular, if the devices are controlling critical infrastructure, sometimes reliability could be an issue, especially during poor weather conditions, which is when utilities would have the most outages and need the information the most [118]. Also, during emergencies, cellular networks can get overloaded and cause network congestions which could cause a challenge if trying to communicate to the device [118]. All of this also increases costs for utilities because it requires them to build their own private network. For mesh networks, there are issues with how much capacity that these networks can handle [118]. Wireless mesh networks are also known to fade their signals and can have interference easily [118]. In rural areas, there is also not enough coverage with smart meters because they are too far apart and the more devices that they must travel data to, there is a higher chance of routing failures [118].

Fiber Optics: One of the best options to send information over the network is to user fiber optic equipment, but there are still limitations with fiber optics [118]. One of the biggest limitations is that installing a fiber-optic network can be very expensive [118]. Also, most of metering applications are constrained by their hardware that require only narrowband communications, where fiber optics use wideband [118]. Fiber optics could be used, but then they would have to install devices that can convert to something the metering devices could connect to.

There are many challenges with implementing IoT in energy systems that utilities will face. Since most utilities don't have advanced technology, it will require that more people or consultants be hired to help support these different networks. There are a lot of challenges in securing the data and sending the data on a medium that works well. The biggest challenge that a lot of the utilities are going to face is the cost to implement a solution, from different hardware costs to having the proper staff.

As the number of smart cities is increasing so it will the number of people, vehicles, sensors, actuators, networks infrastructures in them. Those cities will not be populated only by the people that are very technical and able to use technology efficiently. This presents a problem, how do people that are not technologically literature learn about it and how to use modern technologies. One of the options could be to provide a training to everyone who needs it, but where those funds will come from? Furthermore, can a smart city require its citizens to have certain amount of technical knowledge for basic use of the application and if they do, who will provide the devices in case if they do not have enough funds to purchase them. Will being technologically literature be a norm to live in a smart city in the future, or researchers, countries and governments will find a solution to this. It will be something that smart cities will be facing in the future. On the other hand, cities such as Dubai, Tokyo and Singapore are a good examples of fast pace growth where they attract more young people to live and work in them. Citizens of these cities are driven to use its convenience and usability of the technology so they can focus on other aspects of life and spend more time doing what they want. A lot of times residents of smarts cities do not even have to go out from the houses/apartments for extended periods of time just because everything can be done from their smart devices. This situation creates another problem that can be broken down on two different levels, scalability and security.

Scalability challenges in smart cities: As history have shown, the problem of overpopulating a city creates many difficulties and challenges sometimes solvable and sometimes not for its residents, companies and different institutions residing in those cities. This dates to when the cities were built, and architects did not encounter the growth from just a few thousand people to a multimillion people city. Problems in infrastructure such as water systems, energy systems, roads, buildings, parking places become a big concern. To mitigate the problems architects and engineers try their best to assess the situation, fix it and plan for an expansion of the city based on analytics from previous years. This can be challenging not only because of the price of the projects but as well as physical space in the cities. For example, if larger diameter water pipes are needed, will there be enough space to put them in places of existing without interrupting anything else or new routes will need to be found.

A similar situation of not having enough physical space for the network infrastructures applies where buildings that are not built in mind to have massive amounts of network cables and sever rooms, are forced to accommodate for it because of the devices in the building needed to be connected to the networks. With higher speeds and higher bandwidths of newer technologies, new infrastructure is required. Decades or more of network infrastructures needs to be replaced, which a lot of times has a high cost of implementation and time. Time is very crucial in projects such as this because technologies are evolving quickly, and contractors can run into a problem of still installing the same infrastructure when new technologies are released.

Security challenges in smart cities: The biggest concern that faces not only a smart city but every IoT device is security and privacy. A lot of devices in smart cities are not built with security in mind but to be functional and do the intended job efficiently over long periods of time. Market needs for enormous amounts of IoT devices does not give industries enough time to check for the problems and vulnerabilities on the devices before they put them in production. Situations like this leave a big gap in security and those gaps are usually bridged by major firmware or operating system updates. These unknow problems are only discovered by developers of the product if honest users report them the manufacturer of the product. On the flip side malicious users can exploit a vulnerability in the system or even sell it to third party for extended periods of time without anyone knowing. This allows malicious users to be able to break into these devices and manipulate them at their will. Some might agree that having access to those devices cannot do much damage or that information is not valuable but is that really a truth? A lot of times data from the sensors and devices can be used by third parties for targeted advertising of the user, breached data of the user can be sold to someone to whom it has value and wants to do harms. On a bigger scale, if a system or a database of the smart city is breached this can cause massive outages in electricity, water supplies, etc. If traffic infrastructure in smart city is vulnerable it can cause massive delays in transportation. Such incident can delay grocery and perishable item delivery which can cause them to get spoiled and no longer be usable.

Moreover, if databases that hold sensitive information such as credit cards and social security numbers get exposed because they are used to identify users with devices which can cause massive privacy issues and mistrusts between customers and merchants. Incidents like this can have permanent implications on user lives that may never be resolved. [51]

Considering all these challenges researchers and data scientists are working hard to improve all these technologies and solve problems while also competing with societal expectations, malicious users and deadlines that demand of the products put on them.

7. Summary

As this paper presented segments of the current technologies and its challenges in different areas of IoT, it also abridged common architectures utilized in these systems. Sensors, actuators, technologies that process data and communication systems are what we know to be the corner stones of and IoT architecture. The implementation of architectures can differ depending on the complexity of the system and its requirements to operate as intended. The decision of which architecture to integrate greatly rest on a few variables such as the physical environment, data throughputs, reliability and security. Environments including mines and the ground can require multiple complex components to be implemented in order to get a reliable connection as compared to an open field in agricultural IoT. On the other hand, the distance might not be of great importance to the systems in healthcare IoT, where security is the major role. To maintain the integrity of the information in environments with sensitive data, the processing power of the device needs to be able to support strong encryption methods which involves more powerful chips. Revising all these different architectures this paper also presented some of the most common ways to implement IoT systems in given environments. With the aim of achieving balance between the cost of implementation and the best performance, different wireless communication systems are utilized. These wireless technologies can be divided into long range, medium range and short-range communication methods based on the distance that they can transfer information efficiently over. Technologies such as LoRaWAN, NB-IoT, SigFox and other low power networks fall under long range communication methods and they specify distances in kilometers. Whereas, Wi-Fi resides in medium range because the distance that it can transmit over is higher than in Bluetooth, NFC and RFID, which are considered short range communication systems. Although the diversity in wireless systems allow better flexibility there are a lot of challenges in IoT technologies including insecurity of the devices and scalability. The lack of security measures and the vulnerability within the devices came due to manufacturers massively producing new units and pushing them on the market without appropriate security testing. In terms of scalability engineers are seeking compatibility across different IoT platforms and among different technologies. Over the last few years there have been noticeable improvements in terms of scalability. Lastly, with the increasing numbers of IoT devices throughout industries and the evidence of its convenience, it is safe to say there is an ever-increasing reality in our direction towards each consumer having constant engagement with the Internet of Things and its benefits.

References

1. (2018, April 1). IoT architecture: building blocks and how they work. Retrieved September 8, 2019, from https://www.scnsoft.com/blog/iot-architecture-in-a-nutshell-and-how-it-works

2. (n.d.). Power Management Techniques for Low-Energy IoT Devices. Retrieved from https://www.avnet.com/wps/portal/us/resources/technical-articles/article/iot/power-management-techniques-for- low-energy-iot-devices/
3. (n.d.) IBISWorld, Inc, Industry Market Research, Reports, and Statistics. IBISWorld. Available at: https://clients1.ibisworld.com/reports/us/industry/default.aspx?entid=100
4. 2019. Cost to Build a Net-Zero Energy Home. 24h Site Plans for Building Permits: Site Plan Drawing & Drafting Service. Available at: https://www.24hplans.com/cost-to-build-a-net-zero-energy-home/.
5. 2019. IoT Sensors & Actuators: 2019 List of Sensor and Actuator Types and Manufacturers. Postscapes. Available at: https://www.postscapes.com/trackers/video/the-internet-of-things-and-sensors-and-actuators/.
6. 2019. Sigfox. Wikipedia. Available at: https://en.wikipedia.org/wiki/Sigfox
7. 2019. Smart meter. Wikipedia. Available at: https://en.wikipedia.org/wiki/Smart_meter
8. 2019. Zero-energy building. Wikipedia. Available at: https://en.wikipedia.org/wiki/Zero-energy_building.
9. A. Chehri, P. Fortier, P.M. Tardif, Security monitoring using wireless sensor networks, in: Communication Networks and Services Research, 2007—CNSR’07, May 2007, pp. 13–17.
10. Akash, P. (no date) *What is the Range of Bluetooth? How Can It Be Extended?* Available at: https://www.scienceabc.com/innovation/what-is-the-range-of-bluetooth-and-how-can-it-be-extended.html (Accessed: 13 September 2019).
11. Alam, N., A. T. Balaei, and A. G. Dempster (2013). “Relative position- ing enhancement in VANETs: A tight integration approach”. In: IEEE Trans. Intell. Trasp. Syst. 14.1, pp. 47–55.
12. Aleksandrova, M. (2019, March 11). How IoT is Transforming the Energy Industry. Retrieved from https://easternpeak.com/blog/how-iot-is-transforming-the-energy-industry/
13. Almotiri, Sultan; Khan, Murtaza and Alghamdi, Mohammed. (2016), Mobile Health (m-Health) System in the Context of IoT, 2016 4th International Conference on Future Internet of Things and Cloud Workshops, 10.1109/W-FiCloud.2016.24, pg. 39-42.
14. Al-Turjman, F., Abujubbeh, M. (2018) ’Smart Meters for the Smart-Cities’ Grid’. *Intelligence in IoT-Enabled Smart Cities*. CRC Press, Boca Raton, pp. 63–90. https://doi.org/10.1201/9780429022456-5
15. Al-Turjman, F., Alturjman, S. (2018) ‘Intelligent UAVs for Multimedia Delivery in Smart-Cities’ Applications’, *Intelligence in IoT-Enabled Smart Cities*. CRC Press, Boca Raton, FL : Taylor & Francis, pp. 143–166. https://doi.org/10.1201/9780429022456-8
16. Anagnostopoulos, T., Zaslavsky, A., Kolomvatsos, K., Medvedev, A., Amirian, P., Morley, J., Hadjieftymiades, S., 2017. Challenges and Opportunities of Waste Management in IoT-Enabled Smart Cities: A Survey. IEEE Trans. Sustain. Comput. 2, 275–289. https://doi.org/10.1109/TSUSC.2017.2691049
17. Andión, Javier, Navarro, José, López, Gregorio, … C., J. (2018, December 2). Smart Behavioral Analytics over a Low-Cost IoT Wi-Fi Tracking Real Deployment. Retrieved from https://www.hindawi.com/journals/wcmc/2018/3136471/
18. Anon, THREAD CERTIFIED PRODUCTS. What is Thread. Available at: https://www.threadgroup.org/what-Is-thread [Accessed October 10, 2019].

19. Armstrong, S. (2012) *Which RFID Frequency is Right for Your Application?* Available at: https://blog.atlasrfidstore.com/which-rfid-frequency-is-right-for-your-application (Accessed: 13 September 2019).

20. Asim, Makkad (2017), A Survey on Application Layer Protocols for Internet of Things (IoT), International Journal of Advanced Research in Computer Science, Volume 8, No. 3, March – April 2017, pg. 996-1000.

21. Baker, Stephanie and Xiang, Wei (2017), Internet of Things for Smart Healthcare : Technologies, Challenges, and Opportunities, IEEE Access.

22. Ball, K. Lyon, D. and Haggerty, K. (2012). *Routledge Handbook of Surveillance Studies.* New York: Routledge. [Accessed 8 Sep. 2019].

23. Bassi, A. (2016) 'Looking at smart cities with an historical perspective', in: *Designing, developing, and facilitating smart cities*. Springer Berlin Heidelberg, New York, NY.

24. Basu, S., Pramanik, S., Dey, S., Panigrahi, G. and Jana, D.K., 2019. Fire monitoring in coal mines using wireless underground sensor network and interval type-2 fuzzy logic controller. *International Journal of Coal Science & Technology*, pp.1-12.

25. Bazzi, A. et al. (2019). "Survey and Perspectives of Vehicular Wi-Fi versus Sidelink Cellular-V2X in the 5G Era". In: future internet 11, pp. 122– 141.

26. Beaver, M. (2016). *The Implications of RFID Technology in University ID cards.* [online] mst.edu. Available at: https://scholarsmine.mst.edu/peer2peer/vol1/iss1/3?utm_source=scholarsmine.mst.edu%2Fpeer2peer%2Fvol1%2Fiss1%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages [Accessed 1 Sep. 2019].

27. Bedi, Guneet & Venayagamoorthy, Ganesh & Singh, Rajendra. (2016). Navigating the challenges of Internet of Things (IoT) for power and energy systems. 1-5. 10.1109/PSC.2016.7462853.

28. Benyó, B., Sódor, B., Doktor, T. and Fördős, G. (2012). *University life in contactless way - NFC use cases in academic environment.* IEEEXplore. Available at: 10.1109/INES.2012.6249887 [Accessed 8 Sep. 2019].

29. Bong, D.B.L., Ting, K.C., Lai, K.C. (2008) 'Integrated Approach in the Design of Car Park Occupancy Information System (COINS)'. *IAENG International Journal of Computer Science 35.*

30. Bonomi, F. (2013). "The smart and connected vehicle and the Internet of Things". In: WSTS 2013.

31. Bourque, B. (2014, August 16). This is how Bluetooth works, and no, it's not by magic . Retrieved from https://www.digitaltrends.com/mobile/how-does-bluetooth-work/

32. Brik, B. et al. (2013). "Oken-based clustered data gathering protocol (TCDGP) in vehicular networks". In: Wireless Communications and Mobile Computing

33. Bryant, Meg (Sept 2018), Hackers exploit data in error messages to attack connected medical devices, report finds, https://www.healthcaredive.com/news/hackers-exploit-data-in-error-messages-to-attack-connected-medical-devices/533329/.

34. Cai, H., Xu, B., Jiang, L. and Vasilakos, A.V., 2016. IoT-based big data storage systems in cloud computing: perspectives and challenges. *IEEE Internet of Things Journal*, *4*(1), pp.75-87.

35. Cao, Y. et al. (2015). "A reliable and efficient encounter-based routing frame- work for delay/disruption tolerant networks". In: IEEE Sensors J. 15.7, pp. 4004–4018.

36. Caragliu, A., del Bo, C. and Nijkamp, P. (2011) 'Smart cities in Europe', *Journal of Urban Technology*, 18(2), pp. 65–82. doi: 10.1080/10630732.2011.601117.
37. Challenges of the Internet of Things (IoT) in Energy. Retrieved September 12, 2019, from https://www.electrigence.com/challenges-of-the-internet-of-things-iot-in-energy/
38. Chang, W., H. Lin, and B. Chen (2008). "TrafficGather: An efficient and scalable data collection protocol for vehicular Ad-hoc networks". In: Consumer communications and networking conference, pp. 365–369.
39. Chatschik Bisdikian, I. C. (2001) 'An Overview of the Bluetooth Wireless Technology'. Available at: http://www.di-srv.unisa.it/~vitsca/RC-0809I/pdf00004.pdf.
40. Chew, C. B., Mahinderjit-Singh, M., Wei, K. C., Sheng, T. W., Husin, M. H., and Malim, N. H. A. H. (2015). *Sensors-enabled Smart Attendance Systems Using NFC and RFID Technologies.* [online] researchgate.net. Available at: https://www.researchgate.net/profile/Natalie_Walker4/publication/301655181_Volume_5_Issue_No_1_-_International_Journal_of_New_Computer_Architectures_and_their_Applications_IJNCAA/links/5720586908aefa64889a92ef/Volume-5-Issue-No-1-International-Journal-of-New-Computer-Architectures-and-their-Applications-IJNCAA.pdf#page=22 [Access 7 Sep. 2019].
41. Chiara, B. (2011) 'Sensor Networks with IEEE 802.15.4 systems'. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-642-17490-2.pdf. [41]
42. CHRIS, H. (2019) *Bluetooth 5.1: What's New and Why It Matters*. Available at: https://www.howtogeek.com/403606/bluetooth-5.1-whats-new-and-why-it-matters/ (Accessed: 13 September 2019).
43. Contreras-Castillo, J., S. Zeadally, and Ibanez (2016). "A seven-layered model architecture for Internet of Vehicles". In: Journal of Information and Telecommunication 1.1, pp. 4–22.
44. Corser, G. P., H. Fu, and A. Banihani (2016). "Evaluating location privacy in vehicular communications and applications". In: IEEE Trans. Intell. Transp. Syst. 17.9.
45. Coskun, V., Ozdenizci, B. and Ok, K. (2012) 'A Survey on Near Field Communication (NFC) Technology'. Available at: https://link.springer.com/content/pdf/10.1007%2Fs11277-012-0935-5.pdf.
46. Darwish, D, (2015). Improved Layered Architecture for Internet of Things, International Journal of Current Advanced Research (IJCAR), v.4, pg. 214–223.
47. Daube, Nitzan (2019), Regulating the IoT: Impact and new considerations for cybersecurity and new government regulations, https://www.helpnetsecurity.com/2019/04/11/iot-regulation-2/.
48. De Gennaro, G., Dambruoso, P.R., Loiotile, A.D. et al. (2014). *Indoor air quality in schools.* Environ Chem Lett. Available at: https://doi.org/10.1007/s10311-014-0470-6 [Access 8 Sep. 2019].
49. Djelouat, Hamza; Amira, Abbes and Bensaali, Faycal (2018), Compressive Sensing-Based IoT Applications: A Review Journal of Sensor and Actuator Networks, 2018, 7, 45.
50. Dohare, Y.S., Maity, T., Das, P.S. and Paul, P.S., 2015. Wireless communication and environment monitoring in underground coal mines–review. IETE technical Review, 32(2), pp.140-150.

51. Elmaghraby, A. S. and Losavio, M. M. (2014) 'Cyber security challenges in smart cities: Safety, security and privacy', *Journal of Advanced Research*. Elsevier, 5(4), pp. 491–497. doi: 10.1016/j.jare.2014.02.006.
52. Energy, U.S.D.of, 2013. What Is the Smart Grid? YouTube. Available at: https://www.youtube.com/watch?v=JwRTpWZReJk.
53. Enugala, V. (2018). *Internet of Things - based Smart Classroom Environment*. IEEEXplore. [online] Available at: https://ieeexplore-ieee-org.ezproxy.lib.purdue.edu/stamp/stamp.jsp?tp=&arnumber=8745883 [Accessed 3 Sep. 2019].
54. Evangelatos, O., Samarasinghe, K., & Rolim, J. (2013, May). Syndesi: A Framework for Creating Personalized Smart Environments Using Wireless Sensor Networks. Retrieved from https://www.researchgate.net/publication/261075252_Syndesi_A_Framework_for_Creating_Personalized_Smart_Environments_Using_Wireless_Sensor_Networks
55. Evangelatos, O., Samarasinghe, K., & Rolim, J. (n.d.). Evaluating Design Approaches For Smart Building Systems. Retrieved from http://tcs.unige.ch/lib/exe/fetch.php/user/evaluating.design.approaches.for.smart.building.systems.pdf?id=user%3Aevangela&cache=cache
56. F, Adib., & D, Katabi. (2013, August). See through walls with WiFi! Retrieved from https://www.scopus.com/record/display.uri?eid=2-s2.0-84891595310&origin=inward&txGid=543a3b9179a5d5921b369350688d07e2
57. Fazio, M., A. Puliafito, and M. Villari (2014). "A new architecture to exploit sensin capabilities in smart cities". In: International Journal of Web and Grid Services 10.2, pp. 114–138.
58. Fernandez-Anez, V. (2016) 'Stakeholders Approach to Smart Cities: A Survey on Smart City Definitions', *Alba, E., Chicano, F., Luque, G. (Eds.), Smart Cities*. Springer International Publishing, Cham, pp. 157–167. https://doi.org/10.1007/978-3-319-39595-1_16
59. Fogue, M. et al. (2014). "Securing Warning Message Dissemination in VANETs Using Cooperative Neighbor Position Verification". In: IEEE Trans. Veh. Technol. 64.6, pp. 2538–2550.
60. Gaur, A., Scotney, B., Parr, G., McClean, S. (2015) 'Smart City Architecture and its Applications Based on IoT'. *Procedia Computer Science 52*, 1089–1094. https://doi.org/10.1016/j.procs.2015.05.122
61. George, B., J. Kang, and S. Shekhar (2009). "Spatio-temporal sensor graphs (stsg): A data model for the discovery of spatio-temporal patterns". In: Intelligent Data Analisis 13.3, pp. 457–475.
62. Ghafoor, K. Z. et al. (2013). "Beaconing approaches in vehicular ad hoc networks: A survey". In: Wireless Pers. Commun. 73.3, pp. 885–912.
63. Goodwins, R. (2018) *Next-generation 802.11ax wi-fi: Dense, fast, delayed | ZDNet*. Available at: https://www.zdnet.com/article/next-generation-802-11ax-wi-fi-dense-fast-delayed/ (Accessed: 13 September 2019).
64. Goul, Rick Gould (January 2019), Architecting a Connected Future, https://www.iso.org/news/ref2361.html
65. GSMA (2016), "3GPP Low Power Wide Area Technologies (white paper)".
66. Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013). *Internet of Things (IoT): A vision, architectural elements, and future directions.* Future Generation Computer System. Available at: https://doi.org/10.1016/j.future.2013.01.010

67. Hameed, Sufian; Khan, Faraz Idris and Bilal Hameed (2019), Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review, Journal of Computer Networks and Communications, Volume 2019, Article ID 9629381, 14 pages.

68. Hashemi, S. H., & Kamps, J. (2018, October). Exploiting behavioral user models for point of interest recommendation in smart museums. Retrieved from https://www.researchgate.net/publication/328127785_Exploiting_behavioral_user_models_for_point_of_interest_recommendation_in_smart_museums

69. He, Z. and H. Zhang (2014). "Density adaptive urban data collection in vehicular sensor networks". In: Journal of Networks 9.8, pp. 1993–2002. Huang, J. et al. (2012). "A close examination of performance and power characteristics of 4G LTE networks". In: 10th International Conference on Mobile Systems, pp. 225–238.

70. Hollands, R.G. (2008) 'Will the real smart city please stand up?: Intelligent, progressive or entrepreneurial?'. *City 12*, 303–320. https://doi.org/10.1080/13604810802479126

71. Hua, Liu; Junguo, Zhang and Fantao, Lin, (February 2014), Internet of Things Technology and its Applications in Smart Grid, TELKOMNIKA Indonesian Journal of Electrical Engineering Vol.12, No.2, pg. 940-946.

72. Huang, X. et al. (2016). "Software defined networking with pseudonym systems for secure vehicular clouds". In: IEEE Access 4.1, pp. 3522–3534.

73. Husain Sumra, 2018. US smart meters explained: What is a smart meter and should you opt out? The Ambient. Available at: https://www.the-ambient.com/guides/us-smart-meters-explained-799.

74. Idris, M.Y.I., Leng, Y.Y., Tamil, E.M., Noor, N.M., Razak, Z. (2009) 'Car park system: a review of smart parking system and its technology'. *Information Technology Journal 8*, 101–113.

75. IoT based Smart Tracking of Body Temperature - IoT Blog. (2018, January 23). Retrieved from https://moschip.com/blog/iot/IoT-based-smart-tracking-of-body-temperature

76. Joshi, Naveen (October 2018), Challenges of the Internet of Things, https://www.bbntimes.com/en/technology/challenges-of-the-internet-of-things.

77. Justin, B. (no date) 'The IEEE 802.11 Standardization: Its History, Specifications, Implementations, and Future'. Available at: https://telecom.gmu.edu/sites/default/files/publications/Berg_802.11_GMU-TCOM-TR-8.pdf.

78. Kaiwartya, O. et al. (2014). "Performance improvement in geographic rout- ing for vehicular ad hoc networks". In: Sensors 14.12, pp. 22342–22371. kaiwartya, O. et al. (2016). "Internet of Vehicles: motivation, layered archi- tecture, network model, challenges, and future aspects". In: IEEE Access 4, pp. 5356–5373.

79. Khan, R., Khan, S. U., Zaheer, R., Khan, S. (2012). *Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges*. IEEEXplore. [online] Available at: https://ieeexplore.ieee.org/abstract/document/6424332

80. Khvoynitskaya, S. (2018). Three types of autonomous vehicle sensors in L1–L5 self driving cars. url: https://www.itransition.com/blog/ three-types-of-autonomous-vehicle-sensors-in-self-driving- cars (visited on 09/13/2019).

81. Kokolaki, E., Karaliopoulos, M., Stavrakakis, I. (2012) 'Opportunistically assisted parking service discovery: Now it helps, now it does not'. *Pervasive and Mobile Computing 8*, 210–227. https://doi.org/10.1016/j.pmcj.2011.06.003

82. Kozlov, D.; Veijalainen, J.; Ali, Y., (February 2012), Security and privacy threats in IoT architectures. In Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway, 24–26 February 2012; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2012; pg. 256–262.
83. Layton, J., 2018. How Underground Mining Works. HowStuffWorks Science. Available at: https://science.howstuffworks.com/engineering/structural/underground-mining.htm
84. Lee, S. W. *et al.* (2015) 'Smart water grid: the future water management platform', *Desalination and Water Treatment*. Taylor and Francis Inc., 55(2), pp. 339–346. doi: 10.1080/19443994.2014.917887.
85. Levitt, B.B. & Glendinning, C., 2011. The problems with Smart Grids. Resilience. Available at: https://www.resilience.org/stories/2011-03-23/problems-smart-grids/.
86. Li, M. and Liu, Y., 2007, April. Underground structure monitoring with wireless sensor networks. In *Proceedings of the 6th international conference on Information processing in sensor networks* (pp. 69-78). ACM.
87. Li, X. et al. (2015). "An RSU-coordinated synchronous multi-channel MAC scheme for vehicular ad hoc networks". In: IEEE Access 3.1, pp. 2794– 2802.
88. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W. (2017). *A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications*. IEEEXplore. [online] Available at: https://ieeexplore.ieee.org/abstract/document/7879243 [Accessed 8 Sep. 2019].
89. Liu, N. (Dec. 2011). "Internet of Vehicles your next connection". In: Win- Win Magazine, issue 11, HUAWEI. url: https://www.huawei.com/ en/about- huawei/publications/winwin-magazine/11/HW_110848 (visited on 09/04/2019).
90. Lu, N. et al. (2014). "Connected vehicles: solutions and challenges". In: IEEE Internet of Things Journal 1.4, pp. 289–299.
91. Malik, Hassan; Alam, Muhammad Mahtab; Moullec,Yannick Le and Alar Kuusik (2018), NarrowBand-IoT Performance Analysis for Healthcare Applications, 9th International Conference on Ambient Systems, Networks and Technologies, ANT-2018 and the 8th International Conference on Sustainable Energy Information Technology, SEIT 2018, 8-11 May, 2018, Porto, Portugal, pg. 1077-1083.
92. Masoud M., Jaradat Y., Manasrah A. & Jannoud I. (2019) Sensors of Smart Devices in the Internet of Everything (IoE) Era: Big Opportunities and Massive Doubts. Journal of Sensors. Available at: https://www.hindawi.com/journals/js/2019/6514520/
93. Massimo, D., Not, E. and Ricci, F., 2018, March. User behavior analysis in a simulated iot augmented space. In *Proceedings of the 23rd International Conference on Intelligent User Interfaces Companion* (p. 8). ACM.
94. Matthews, Kayla (December, 2018), 5 Challenges Facing Health Care IoT in 2019, https://www.iotforall.com/5-challenges-facing-iot-healthcare-2019/
95. McCafferty, S., Forfia, D., & McCormick, E. (2019, April 29). EnergyIoT Article 3 – IoT Architecture Big Picture. Retrieved September 4, 2019, from https://www.energycentral.com/c/iu/energyiot-article-3-—-iot-architecture-big-picture
96. McKinsey&Company (2013). The road to 2020 and beyond – What's driving the global automotive industry. url: https : / / www . mckinsey . com / industries / automotive - and - assembly / our - insights (visited on 09/01/2019).

97. Merry, H., 2019. 5 benefits IoT is having on the mining industry. Internet of Things blog. Available at: https://www.ibm.com/blogs/internet-of-things/mining-industry-benefits/

98. Mijac, M., Androcec, D., Picek, R. (2017) 'Smart City Services Driven By Iot: a Systematic Review'. *Journal of Economic and Social Development* 4, 40–50.

99. Mora, N., Grossi, F., Russo, D., Barsocchi, P., Hu, R., Brunschwiler, T., … Ciampolini, P. (2019, July 23). IoT-Based Home Monitoring: Supporting Practitioners' Assessment by Behavioral Analysis. Retrieved from https://www.mdpi.com/1424-8220/19/14/3238/htm

100. Mukherjee S., Bhole K., Sonawane D. (2019) Design and Development of Scalable IoT Framework for Healthcare Application. Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB). ISMAC 2018. Lecture Notes in Computational Vision and Biomechanics, vol 30. Springer, Cham.

101. Namiot, D. (2019). On Internet of Things Education. *20TH CONFERENCE OF FRUCT ASSOCIATION*. [online] Available at: https://ieeexplore-ieee-org.ezproxy.lib.purdue.edu/stamp/stamp.jsp?tp=&arnumber=8071327&tag=1 [Accessed 4 Sep. 2019].

102. Nelson, Patrick (Feb 2019), Power over Wi-Fi: The end of IoT-sensor batteries? Network World | FEB 21, 2019, https://www.networkworld.com/article/3342417/power-over-wi-fi-the-end-of-iot-sensor-batteries.html

103. NRG Energy, Inc. (2018, February 18). How IoT Is Transforming the Energy Industry. Retrieved September 12, 2019, from https://www.nrg.com/insights/innovation/how-iot-is-transforming-the-energy-industry.html

104. OICA (2015). Number of passenger cars and commercial vehicles in use worldwide from 2006 to 2014. url: http://www.oica.net/category/ vehicles-in-use/ (visited on 09/01/2019).

105. Palazzi, C., F. Pezzoni, and P. Ruiz (2012). "Delay-bounded data gathering in urban vehicular sensor networks". In: Pervasive and Mobile Computing 8.2, pp. 180–193.

106. Prasanna, J.L., Lavanya, D. and Kumar, T.A., 2017, October. Condition monitoring of a virtual solar system using IoT. In 2017 2nd International Conference on Communication and Electronics Systems (ICCES) (pp. 286-290). IEEE.

107. Pratt, K. Mary, (Feb 2019), Top Challenges of IoT adaptation in the enterprise, https://internetofthingsagenda.techtarget.com/feature/Top-challenges-of-IoT-adoption-in-the-enterprise

108. Preuveneers, D. and Y. Berbers (2014). "SAMURAI: A streaming multi- tenant context-management architecture for intelligent and scalable Internet of things applications". In: International conference on intelligent environments (IE), pp. 226–233.

109. Purdue.edu. (2019). *About AirLink - Airlink - Purdue University*. [online] Available at: https://www.purdue.edu/airlink/about.php [Accessed 5 Sep. 2019].

110. Purdue.edu (2019). *Innovative Learning*. [online] Available at: https://www.purdue.edu/innovativelearning/ [Accessed 3 Sep. 2019].

111. Qureshi, M. A. et al. (2015). "A survey on obstacle modeling patterns in radio propagation models for vehicular ad hoc networks". In: Arabian J. Sci. Eng. 40.5, pp. 1385–1407.

112. Rahman, M. (2016). *ICT and Internet of Things for Creating Smart Learning Environment for Students at Education Institutes in India.* IEEExplore. [online] Available at: https://ieeexplore-ieee-org.ezproxy.lib.purdue.edu/stamp/stamp.jsp?tp=&arnumber=7508209 [Accessed 27 Aug. 2019].

113. Ranjan, A., Sahu, H.B. and Misra, P., 2019. MineSense: sensing the radio signal behavior in metal and non-metal underground mines. *Wireless Networks*, *25*(6), pp.3643-3655.

114. RF Wireless World. 2019. Arduino Sensors. [ONLINE] Available at: https://www.rfwireless-world.com/. [Accessed 1 September 2019].

115. Rodier, C.J., Shaheen, S.A. (2010) 'Transit-based smart parking: An evaluation of the San Francisco Bay area field test'. *Transportation Research Part C: Emerging Technologies* 18, 225–233. https://doi.org/10.1016/j.trc.2009.07.002

116. Rudolph, G and U. Voelzke (2017). Three types of autonomous vehicle sen- sors in L1–L5 self driving cars. url: https://www.fierceelectronics. com/components/three-sensor-types-drive-autonomous-vehicles (visited on 09/13/2019).

117. Said, O.; Masud, M., (2013), Towards Internet of things: Survey and future vision. International Journal for Computer Network. 2013, v.5, pg. 1–17.

118. Saleem, Yasir & Crespi, Noel & Rehmani, Mubashir Husain & Copeland, Rebecca. (2019). Internet of Things-aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions. IEEE Access. PP. 10.1109/ACCESS.2019.2913984.

119. Seneviratne, P. (2019) 'Beginning LoRa Radio Networks with Arduino', in. Available at: https://link.springer.com/content/pdf/10.1007%2F978-1-4842-4357-2.pdf.

120. Serdaroglu, K. and Baydere, S. (2015). WiSEGATE: Wireless Sensor Network Gateway framework for internet of things. *Wireless Networks*, 22(5), pp.1475-1491.

121. Sethi, P.; Sarangi, S.R., (2017), Internet of Things: Architectures, Protocols, and Applications, Journal of Electrical and Computer Engineering, 2017, 9324035.

122. Shah, Syed Tauhid Ullah & Yar, Hekmat & Khan, Izaz & Ikram, Muhammad. (2019). Internet of Things-Based Healthcare: Recent Advances and Challenges. 10.1007/978-3-319-96139-2_15.

123. Shahinzadeh, Hossein & Moradi, Jalal & Gharehpetian, Gevork & Nafisi, Hamed & Abedi, Mehrdad. (2019). IoT Architecture for Smart Grids. 22-30. 10.1109/IPAPS.2019.8641944.

124. Sinha, R. S., Wei, Y. and Hwang, S. H. (2017) 'A survey on LPWA technology: LoRa and NB-IoT', *ICT Express*. Korean Institute of Communications Information Sciences, pp. 14–21. doi: 10.1016/j.icte.2017.03.004.

125. Sommer, C. et al. (2015). "How shadowing hurts vehicular communications and how dynamic beaconing can help". In: IEEE Trans. Mobile Compute. 14.7, pp. 1411–1421.

126. Soua, A. and H. Afifi (2013). "Adaptive data collection protocol using reinforcement learning for VANETs". In: 9th International Wireless communication and mobile computing conference (IWCMC), pp. 1040–1045.

127. Steenberghen, T., Dieussaert, K., Maerivoet, S., Spitaels, K. (2012) 'SUSTAPARK: An Agent-based Model for Simulating Parking Search'. *Journal of the Urban & Regional Information Systems Association* 24.

128. Sun, Z. and Akyildiz, I.F., 2010. Channel modeling and analysis for wireless networks in underground mines and road tunnels. *IEEE Transactions on communications*, *58*(6), pp.1758-1768.

129. Taft, J., Melton, R., & Hardin, D. (2019, September 2). Next-Gen Grid Architecture: A prerequisite for grid modernization. Retrieved September 12, 2019, from https://www.power-grid.com/2019/04/09/next-gen-grid-architecture-a-prerequisite-for-grid-modernization/#gref

130. Techbriefs Media Group, 2018. Smart Sensor Technology for the IoT. Tech Briefs. Available at: https://www.techbriefs.com/component/content/article/tb/features/articles/33212.

131. Temker, R., Gupte, M. and Kalgaonkar, S. (2016). *Internet of Things for Smart Classrooms.* International Research Journal of Engineering and Technology (IRJET). Available at: https://pdfs.semanticscholar.org/e9b5/6e979bd90ef86ced36a92945b187810761c9.pdf [Accessed: 9 Sep. 2019].

132. The Dayton Power and Light Company (6AD) 'Save on Your Energy Costs with a Smart Thermostat from Dayton Power and Light', *Business Wire (English)*, 2017 . Available at: http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=bizwire.c79467153&site=ehost-live (Accessed: 8 September 2019).

133. Tyagi, A. K. and N. Sreenath (2015). "Location privacy preserving techniques for location-based services over road networks". In: Proc. IEEE

134. Vuran, M.C., Salam, A., Wong, R. and Irmak, S., 2018. Internet of underground things in precision agriculture: Architecture and technology aspects. *Ad Hoc Networks*, *81*, pp.160-173.

135. Wan, J. et al. (2014). "Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions". In: IEEE Communications Magazine 58.2, pp. 106–113.

136. Weinschenk, C. (2015, November 11). Energy Management: The Internet of Things Changes Everything. Retrieved September 3, 2019, from https://www.energymanagertoday.com/energy-management-the-internet-of-things-changes-everything-0120273/

137. Wellens, M., B. Westphal, and P. Mahonen (2007). "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios". In: Proceedings of 2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring, pp. 1167–1171.

138. Which?, 2019. How do smart meters work - Which? advice. YouTube. Available at: https://www.youtube.com/watch?v=f_a3c_EbCSo

139. Wilson C., Hargreaves T. & Hauxwell-Baldwin R. (2017) Benefits and Risks of Smart Home Technologies. Energy Policy. Available at: https://www.sciencedirect.com/science/article/pii/S030142151630711X

140. Wu, Taiyang; Wu, Fan; Redoute, Jean-michel; and Yuce, Mehmet Rasit (June, 2017), An Autonomous Wireless Body Area Network Implementation Towards IoT Connected Healthcare Applications, IEEE Access, v.5, 2017.

141. Yang, F. et al. (Oct. 2014). "An overview of Internet of Vehicles". In: China Communications 11.10, pp. 1–15.

142. Yang, Y. and Yu. K. (2016). *Construction of Distance Education Classroom in Architecture Specialty Based on Internet of Things Technology.* International Journal of Emerging Technologies in Learning (iJET), 11(05), p.56. [Accessed 7 Sep. 2019].

143. Yang H., Lee W. & Lee H. (2018) IoT Smart Home Adoption: The Importance of Proper Level Automation. Journal of Sensors. Available at: https://www.hindawi.com/journals/js/2018/6464036/

144. Yao, J. et al. (2011). "Improving cooperative positioning for vehicular net- works". In: IEEE Trans. Veh. Technol. 60.6, pp. 2810–2823.

145. Yarkan, S., Guzelgoz, S., Arslan, H. and Murphy, R.R., 2009. Underground mine communications: A survey. *IEEE Communications Surveys & Tutorials*, *11*(3), pp.125-142.

146. Ying, B., D. Makrakis, and H. T. Mouftah (2013). "Dynamic mix-zone for location privacy in vehicular networks". In: IEEE Commun. Lett. 17.8, pp. 1524–1527. [146]

147. Yusof, R. J., Qazi, A. and Inayat, I. (2017) *'Student Real-Time Visualization System in Classroom Using RFID Based on UTAUT Model'*, International Journal of Information and Learning Technology, 34(3), pp. 274–288. Available at: http://search.ebscohost.com.ezproxy.lib.purdue.edu/login.aspx?direct=true&db=eric&AN=EJ1141033&site=ehost-live [Accessed: 8 September 2019].
148. Zeadally, S. et al. (2012). "Vehicular ad hoc networks (VANETS): status, results, and challenges". In: Telecommunication Systems 50, pp. 217– 241.
149. Zhan, H. (2019). *5G Will Hit A Wall, Literally, In 2019*. [online] IT Infrastructure Advice, Discussion, Community - Network Computing. Available at: https://www.networkcomputing.com/networking/5g-will-hit-wall-literally-2019.
150. Zhang, Q., Huang, T., Zhu, Y., Qiu, M. (2013) 'A Case Study of Sensor Data Collection and Analysis in Smart City: Provenance in Smart Food Supply Chain'. *International Journal of Distributed Sensor*