ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/351554927

Internet of things (IoT)

Chapter · May 2021
DOI: 10.1088/978-0-7503-3663-5ch1

CITATIONS
14

READS
52,390

2 authors, including:

Seifedine Kadry
Noroff University College
847 PUBLICATIONS **10,451** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Big Data in Finance View project

Project Project 1: Learning Analytics View project

All content following this page was uploaded by Seifedine Kadry on 24 May 2021.

The user has requested enhancement of the downloaded file.

IOPscience iopscience.iop.org

This content has been downloaded from IOPscience. Please scroll down to see the full text.

Download details:

IP Address: 45.130.35.123
This content was downloaded on 24/05/2021 at 11:21

Please note that terms and conditions apply.

You may also be interested in:

Radiative Properties of Semiconductors: Global infrastructure for emissivity measurements—examples
N M Ravindra, S R Marthi and A Bañobre

Wearable Sensors: GUI-based software development for sensor data collection, data extraction and data analysis using Python frameworks
S C Mukhopadhyay and T Islam

Research on key technologies of data processing in internet of things
Yangqing Zhu and Peiying Liang

Cognitive IoT incorporating intelligence in building smart environment
Dishari Sarker and S Sumathy

Development of ship structure health monitoring system based on IOT technology
Sujun Yang, Lei Shi, Demin Chen et al.

Research on Internet of Things Data Mining Based on Cloud Computing Platform
Enhong Liao

Review on open source operating systems for internet of things
Zhengmin Wang, Wei Li and Huiliang Dong

Internet of Things in Higher Education: A Study on Future Learning
Hanan Aldowah, Shafiq Ul Rehman, Samar Ghazal et al.

Network Function Virtualization (NFV) based architecture to address connectivity, interoperability and manageability challenges in Internet of Things (IoT)
Shariq Haseeb, Aisha Hassan A. Hashim, Othman O. Khalifa et al.

IOP Publishing

Blockchain in the Industrial Internet of Things

Lakshmana Kumar Ramasamy and Seifedine Kadry

Chapter 1

Internet of things (IoT)

The Internet of Things (IoT) refers to the evolutionary stage of the internet, which makes a global communicating infrastructure between humans and machines. IoT is constructing the global infrastructure which will change the fundamental aspects of our lives, from health services to manufacturing, from agriculture to mining. IoT will offer the necessary facilities of the latest rising artificial intelligence (AI) development. This chapter discusses the overview, characteristics, advantages, disadvantages, common uses, security, trust, privacy and functional view of IoT. Furthermore, this chapter proposes application areas of IoT in detail.

1.1 IoT overview

IoT has grown to be a marketing trend and general news piece. Beyond exaggeration, IoT appeared as a powerful technique with appliances in numerous domains. IoT has origins in multiple former methods: sensor networks, embedded systems and pervasive informatics. Many IoT devices are linked mutually to develop specific purpose schemes; in the global network, they are rarely utilized as public access devices.

An IoT node is a sensor contained hardware piece that broadcasts sensed information to users or any other devices over the internet. IoT nodes embed into industrial equipment, mobile and medical instruments, wireless sensors, and more. Top examples of IoTs are connected smart city, smart industry, smart transport, smart buildings [1], smart energy, smart manufacturing, smart environment monitoring, smart living, smart health, smart food and water monitoring. Figure 1.1 shows the IoT network architecture. This architecture has a lot of IoT sensors for sensing purposes such as temperature, humidity, pressure etc. After sensing, these data are transmitted to a cloud server via an IoT gateway. Furthermore, users can access these data through mobile apps and so on.

Due to the accessibility of low cost and smart devices, the IoT network refers to a smart system. IoT devices operate independently with their hearing and transmission

doi:10.1088/978-0-7503-3663-5ch1

© IOP Publishing Ltd 2021

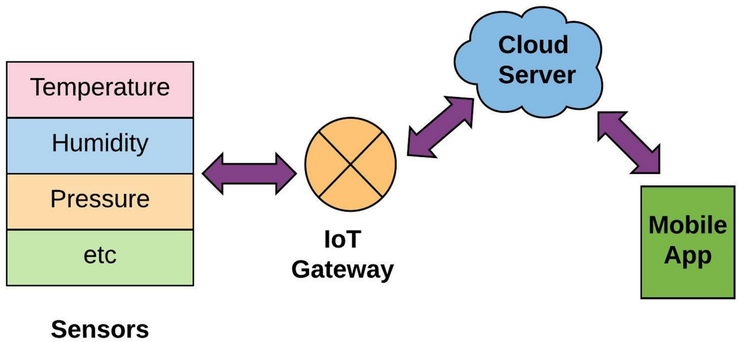


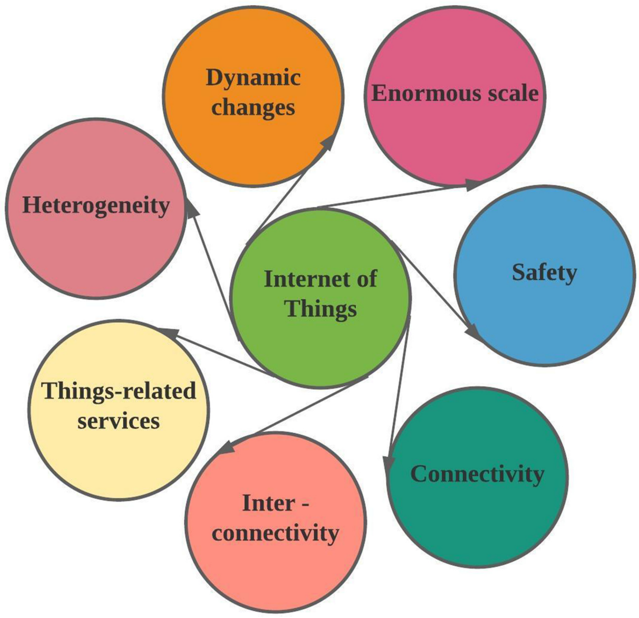
Figure 1.1. IoT network architecture.

abilities. Furthermore, the propagation of IoT provides a lot of benefits but also provides potential threats. An overlooked factor so far is the rise in energy expenditure. IoT nodes are anticipated to always be accessible on other nodes. IoT offers a lot of benefits, including:

- **Locating and tracing abilities**: Customers should be capable of tracking the nodes and locating them in a short amount of time.
- **Ubiquitous information swap**: In IoT where nodes are linked to the internet and where information is transmitted. Ubiquitous means intelligence. Therefore, intelligence sensors collect information and transmit it using a prearranged input.
- **Enhanced power solution**: Customers should be capable of tracking even the strongest node, and the customer should be capable of obtaining the best result.
- **Data and intelligence management**: IoT does not always require providing commands to the instrument; where the node gives intelligence and information previously it can start working and obtains decisions and discovers solutions based on intelligence.
- **Scalability**: IoT should be the measurability, as with any number of IoT nodes above an extensive network all nodes should distinguish uniquely.

Also, numerous significant IoT problems can be identified. These open problems make it clear that the complexity of internet design currently needs significant capabilities to alter.

- **Unprotected authorization/authentication**: The administrator usually presents authentication to verify the customer identity, and the authorization utilizes rewriting or modifying the content for that appliance and the consent that the administrator will give.
- **The technology of server**: The number of IoT nodes over the IoT field increases the demand and the number of IoT node replies, moreover increases simultaneously depending entirely on the server where customers use the



Figurere 1.2. Characteristics of IoT.

interface. The server response to the IoT node demand should be made immediately. There must be no delay in responding to the customer.

- **Management of storage**: A massive quantity of information is created. When connected IoT nodes have a massive quantity of multimedia data transmitted, they have big data and other types of inconsistent files where data is held concerning these IoT nodes, these files do not take much space. Still, many of them should be useable as soon as possible.
- **Data management**: As transmission between nodes is completed, more information is created daily between nodes, and there is more information to be transmitted from one location to another. Consideration should be given to whether specific information is transmitted or not.
- **Security**: Provision of security can be challenging as the automation of nodes has increased, which has generated novel security problems.

1.1.1 IoT essential characteristics

Figure 1.2 shows IoT essential characteristics discussed as follows:

- **Enormous scale**: The number of IoT nodes that require handling and connecting will be a order of magnitude higher than the IoT nodes currently linked to the internet. Of particular importance will be the administration of the information created and its analysis for appliance reasons. It is about content semantics, with content management.
- **Safety**: As customers achieve advantages from IoT, customers should not fail to remember security. As senders and receivers of IoT, they should plan for

security. This encompasses the security of customer information and the security of customer welfare: protecting networks, endpoints, and is a universal message that represents generating a measurable safety model.

- **Dynamic changes**: Device status changes drastically, for instance, sleep and wakefulness, connection and disconnection and content of IoT nodes contain speed and position. Besides, the number of IoT nodes can modify energetically.
- **Heterogeneity**: Various IoT nodes depending on various networks and hardware platforms. They should connect to other nodes via various networks.
- **Connectivity**: This permits IoT to have ease of access and compatibility. Ease of access is obtainable on the network though compatibility, presenting the same capabilities for using and producing content.
- **Services related to things**: IoT can present a lot of services related to things within things restrictions. To present services related to things within things limitations, both techniques in the global and data world will alter.
- **Interconnectivity**: In terms of IoT, anything could be linked to universal data and contact the IoT basic organizational and physical structures.

1.1.2 IoT benefits

Currently, every part of business and lifestyle hopes to realise the benefits of IoT. Figure 1.3 shows a list of a few of the benefits that IoT will provide:

- **Technical enhancement**: Similar techniques and data that enhance consumer observation of IoT facts and enhance IoT node usage, and facilitate the most significant advances in technique. IoT opens up a world of actual data performance and field performance.
- **Enhanced consumer engagement**: Recent statistics have the problem of ambiguity and fundamental errors in precision; also, as mentioned,

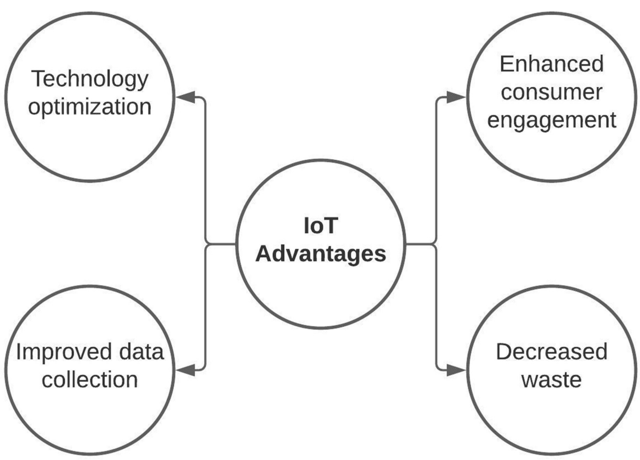


Figure 1.3. Advantages of IoT.

engagement remains are inactive. IoT changes this, attaining a rich and productive engagement, including the spectator.

- **Advanced information compilation**: Today's information compilation undergoes restrictions in plans for practical usage. IoT smashes it down into those gaps and then puts it right where people desire for investigating our planet.
- **Decreased waste**: IoT generates development fields more clearly. Recent statistics provide us with insignificant intelligence, rather IoT presents actuality data that leads to efficient resource management.

1.1.3 IoT drawbacks

IoT provides an inspiring collection of advantages; it moreover provides an essential collection of challenges. Figure 1.4 shows a list of some of its main problems:

- **Security**: IoT generates an environmental scheme for frequently linked nodes contacting networks. Furthermore, the scheme provides minimal regulation despite safety measurements. It protects consumers from different types of hackers [1].
- **Privacy**: IoT expertise presents private information with complete information, not including the involvement of the consumer.
- **Flexibility**: Consumers are worried regarding the elasticity of the IoT scheme for easy integration. The anxiety is about discovering themselves with too many contradictory or protected source codes.
- **Compliance**: IoT, similar to all other technologies in the trade sector, should obey the rules. Its difficulty creates the problem of compatibility seeming like a daunting challenge when many think that typical software compatibility is a war.

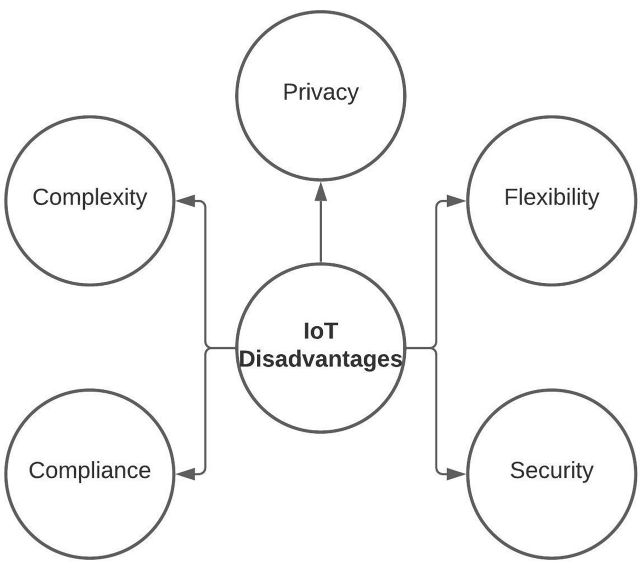


Figure 1.4. Disadvantages of IoT.

- **Complexity**: A few consumers discover that IoT schemes are complicated in the rule of schema, ordering, and storage provided for their usage of numerous techniques and a massive collection of newly permitted techniques.

1.2 IoT common uses

IoT schemes are helpful for many types of appliances:

- Industrial schemes utilize sensors to monitor together with the industry procedures themselves—product excellence—and the condition of the apparatus. A growing number of electric motors, for instance, contain sensors that gather information utilized to forecast future motor breakdowns.
- Smart buildings utilize sensors to discover the positions of persons and the condition of a building. That information can be utilized to regulate ventilation/ air conditioning and lighting schemes to decrease working prices. Smart buildings also utilize sensors to monitor the physical condition of the building.
- Smart cities utilize sensors to monitor persons walking rather than travelling in a vehicle as well as vehicle traffic, and can compile information from smart buildings.
- Vehicles utilize network sensors to monitor vehicle condition and offer enhancement, decrease energy expenditure, and reduce inferior discharges.
- Medical schemes link with a variety of patient monitoring sensors that can be situated at home, in an emergency vehicle, or in a hospital.

There are lots of use cases that assist users in recognizing the needs of the IoT scheme.

Notification system: Messages from IoT devices can be collected and examined. Notices made when certain conditions are met.

Sensor network: The scheme can work definitely as an information collection scheme for the sensor sets.

Reactive system: Study of IoT device sensed information could incite actuators to be accelerated. Users retain a word reactive for schemes that do not execute standard regulatory rules.

Analysis system: Messages from IoT devices are collected and examined, other than in that event, the research is continuing. Research outcomes can be created occasionally.

Event latency: Delays from capturing an event to its receiver cannot be significant for volume-based apps but are significant for online research.

Control scheme: IoT device sensed information is nourishing to regulate the instructions that produce the effects for the actuator. Users may discover the category of non-functional necessities that execute to most IoT schemes. Non-functional necessities in the scheme force non-functional needs on the elements.

Buffer volume and event loss rate: If there are no strict limits on event manufacturing standards, the surroundings can generate multiple events over some time over the scheme. The event loss rate holds the preferred abilities, while buffer volume is a practical need that may directly link to the strength of the elements.

Availability and reliability: As IoT, schemes are dispersed; availability is often utilized to explain dispersed schemes. Reliability may determine across network components instead of total scheme reliability.

Throughput and service latency: Finally, procedures would be executed through maintenance. Users could indicate throughput and delays of maintenance.

A lifetime of service: IoT schemes are always anticipated to contain longevity greater than users anticipate for PC schemes. The lifespan of a scheme or subdivision of a scheme might be longer than that of an element, mainly if a scheme utilizes passive sensors and different elements.

1.3 IoT—security

Security is ultimately seen as a significant necessity for each kind of computer scheme, containing IoT schemes. However, most IoT schemes are significantly safer than standard Windows/Linux/Mac schemes. IoT safety issues arise from a variety of reasons: insufficient hardware safety elements, inadequately created software with broad limitations of susceptibilities, and different safety creation faults.

Unprotected IoT devices generate safety issues for the whole IoT scheme. Since devices generally contain a lifespan of numerous years, an enormous established foundation of vulnerable IoT nodes would cause safety issues in the future. Unprotected IoT schemes create safety issues across the internet. IoT nodes abound; unprotected IoT devices are perfectly suitable for a lot of attacks (especially denial-of-service (DoS)). Consumer details are secure from direct theft; however, the IoT needs to be built, thereby low confidentiality information could not be merely utilized for conjecture about high confidentiality information.

Example: A German article states that attackers have hacked the safety scheme. They disturbed the management scheme, which prevented the furnace from closing correctly, resulting in serious harm. Therefore, users may know the consequence of the assault earlier, determining a suitable defence.

Challenges: Aside from pricing and availability of IoT nodes everywhere, different safety problems cause continual trouble to the IoT shown in figure 1.5:

- **Device similarity**: IoT nodes are well homogeneous. These nodes use a similar communication technique and elements. If one scheme or node is vulnerable from susceptibility, numerous others contain a similar problem.
- **Unexpected activities**: The vast amount of IoT nodes used and their vast list of empowering techniques denotes that these nodes activities in the area may be unexpected. A particular scheme might be well-designed within management systems; however, there are no assurances of how it will communicate with other nodes.
- **Device longevity**: One of the advantages of IoT nodes is long life, but that long life denotes that they can live longer with their node assistance. One can measure the similarity or dissimilarity between this and conventional schemes that have to assist and modernize after a long time, with numerous terminating

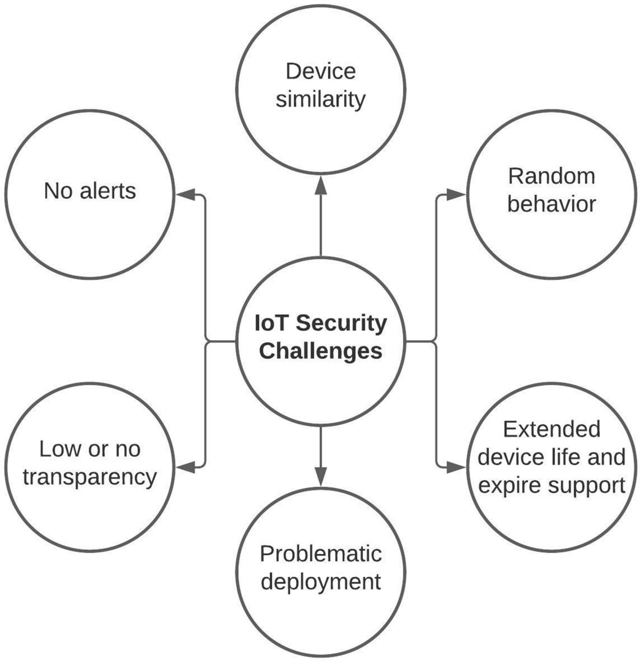


Figure 1.5. Security challenges of IoT.

their utilization. Abandonware and Orphan nodes do not have a similar safety toughness for different schemes because of the emergence of techniques over time.

- **Complex deployment**: One of the primary objectives of IoT is to put superior networks and research where they could not go before. Unexpectedly, this makes a difficulty for physical protection of nodes in these areas that are extreme or only accessible with difficulty.
- **Lack of transparency**: Numerous IoT nodes fail to present clarity in terms of their performance. Consumers are unable to see or use their procedures and can only assume the nodes work correctly. They cannot regulate unnecessary activities or information gathering; moreover, when the producer updates the node, it might carry unnecessary activities.
- **No warnings**: One more purpose of IoT is to offer the best performance in the absence of interruption. This initiates consumer consciousness issues. Consumers are not aware of the nodes or recognize when an unfamiliar thing becomes invalid. Safety violations may continue for a long time in the absence of discovery.

1.3.1 Trust for IoT

A trustworthy structure needs to be able to manage people and equipment as consumers, e.g. it needs to transfer hope to people and to be strongly sufficient to be utilized by types of equipment without DoS attack [2]. The building of hope structures that tackle this necessity will need improvements in fields, for example:

- Lightweight public key infrastructures (PKIs) as a basis for confidence management. Improvements are predicted in hierarchy and cross-certification ideas to allow decisions to deal with the scalable necessities.
- Lightweight key management schemes to allow confidence relations to be set up and to share encryption tools using minimal contact and procedure tools, as well as limited resource nature of numerous IoT nodes.
- Data quality is a necessity for numerous IoT-designed schemes where a set of data that describes data about other information can be utilized to offer IoT information reliable estimation.
- Decentralized and self-configuring schemes are substituted by PKI to set up reliability, for instance, a federated identity, Peer-to-peer (P2P) network.
- Reliability negotiation is a process that permits two parties to discuss routinely, basically a sequence of reliability tenets, the low condition of reliability needed to allow an act of assistance or a data strip.
- Guaranteed techniques for reliable sites contain protocols, software, hardware, etc.
- Access control to avoid information violations. One instance is usage regulation, which is the procedure of guaranteeing the proper use of specific data according to a pre-defined principle, after which the access to data is allowed [3].

1.3.2 IoT privacy

Most of the data in an IoT scheme can be private information; there is a need to assist in anonymous and limited private data management. There are many fields where development is needed:

- Cryptographic technologies that allow secured data to be saved and progressed and distributed, without the data being accessible to third parties.
- Securing the secrecy of the area, where the area can be incorporated into things related to human beings [3, 4].
- Restriction of private data presumption, people may desire to maintain it confidential, by looking at IoT associated transactions.
- Maintaining data as the neighborhood as is feasible utilizing key management and distributed computing.
- A soft identifier application, where consumer identity can be utilized to make a wide variety of different identities for particular appliances. One soft identifier may not build for a particular theme without exposing unnecessary details, which could lead to a violation of confidentiality [4].

1.4 Functional view of IoT

The IoT system indicates to uniquely discoverable devices with their visual presentations in a structure such as the Internet and IoT problem solving that include many elements, for example:

1) IoT local device communication model (a small distance wireless network can be contacted, for instance, installed on a mobile phone or situated in the surroundings of a consumer etc). This model is in responsible for acquiring, monitoring and transmission to remote servers for perpetual storage and research.
2) Local research module and observation processing obtained by IoT nodes.
3) Model to communicate with remote IoT nodes,directly on the internet or possibly by proxy. This model is in charge of observation acquired and transmission to remote servers for perpetual storage and research.
4) Data analytics applications model works on an application server that serves all customers. It takes demands from the web and mobile customers as well as appropriate IoT views as input, implements relevant information executing algorithms and provides output based on skills that will be provided after to consumers.
5) Consumer interface (mobile or web): measurements of the visual representation in the given circumstances and consumer communication, e.g. description of customer enquiries.

1.5 Application domains

IoT application areas identified by the IoT European Research Cluster (IERC) based on the inputs of specialists, reports and studies. Top examples of IoT applications are smart city, smart industry, smart transport, smart buildings, smart energy, smart manufacturing, smart environment monitoring, smart living, smart health, smart food and water monitoring.

Industrial automation and production stressed from the shortlived manufacturing life cycle and the need for short-term marketing in numerous domains. The next-generation of production schemes will be constructed on elasticity and redesigned as an important goal. The new list of IoT appliances presented beneath includes examples of IoT applications in different areas, indicating why IoT is one of the planned technique fashions over the subsequent five years.

1.5.1 Smart industry

Machine-to-machine appliances: Automatic machine diagnostics and asset management.

The liquid level of a tank or vessel: Monitoring fuel and water levels in storage vessels and wells.

Silo volume calculator: Measure of emptiness and weight of merchandise.

Air quality within and around buildings and structures: Supervising of dangerous gas and oxygen quantities within an industrial process plant that manufactures chemicals to guarantee the safety of workers and merchandise [5, 6].

The presence of ozone: Ozone monitoring for the period of dry meat processing in the food industry.

Measurement and monitoring of temperature: Temperature control inside medical refrigerator systems with important ingredients.

1.5.2 Smart mobility and transport

Shipment Quality: Supervising of container openings, vibrations, impacts, or any damage for insurance.

NFC Payment: Enable merchants to get credit or debit card payments online by offering a link to a merchant bank or acquirer based in a place or time required to complete the activities of public transportation, museums, galleries, and so on.

Object Location: Search individual objects in large locations such as repositories or ports.

Monitor the activity of fleet vehicles and assets: Route control of critical assets such as jewels, medical drugs or hazardous materials.

Non-compatibility discovery of storage: Alerting of containers' emission of readily combustible materials close to others holding explosives.

Car management: Car sharing organizations run the usage of vehicles using smartphones with net connections fixed in each car.

Automatic vehicle diagnosis: Data gathering from CAN Bus to transmit a real-time alarm to immediate risks or to offer tips to a person who drives a vehicle.

1.5.3 Smart buildings

Liquid availability: Liquid discovery in data centres, buildings for storing goods and significant construction underground to avert collapse and the process of slow destruction by chemical action.

Access control of perimeter: Selective restriction of access to protected areas and the discovery of human beings in unauthorized areas [3].

Control of indoor climate: Measuring and controlling a physical quantity that expresses hot and cold, equipment for producing light, carbon dioxide in fresh air at ppm and so on.

Preserving culture through art: Condition monitoring within museums and art galleries.

Intrusion prevention system: Discovery of doors and windows openings and breaches to detect intruders, especially into a building with criminal intent.

Residential-irrigation: Smart irrigation and monitoring system.

1.5.4 Smart energy

Installation of photovoltaic: Supervising and enhancing of operation in solar power stations [7].

Grid modernization: Power usage supervising and controlling.

Wind energy converter: Supervising and examining the flow of power from a wind energy converter, as well as two-way contact with smart meters for customers to examine usage patterns.

Radiation rate: Shared calculation of radiation rates in surrounding nuclear power plants to create leak warnings.

Stream: Measuring water force that pushes water through pipes in water flow schemes.

1.5.5 Smart production

Composting: Temperature and humidity management in hay, alfalfa, straw, and so on to deter fungi and various microbiological contaminations.

Intelligent management of manufactures: Controlling stock rotation based on FIFO (First-IN, First-OUT) rules on warehouse shelving and storage to stock replenishment automation.

Descendant care: Controlled breeding in farm animals to guarantee their health and survival [8].

Measurements of toxic gas: Research of air pollution in farm buildings and the discovery of dangerous gases from stables [5, 6].

Tracking animals: Locating and identifying animals that graze in open grazing lands or area in the largest stables.

Telecommuting: Providing workers with technology to allow local offices will decrease costs, increase productive capacity, and increase job opportunities while decreasing staff housing, reducing office maintenance and cleaning, and removing everyday office travel.

Production-line monitoring: Production-line monitoring and managment based on radio-frequency identification (RFID), sensors, video surveillance, remote data sharing and cloud-based solutions that allow production-line information to change to business-based schemes.

1.5.6 Smart environment monitoring

Air contamination: Decreasing CO2 emissions from industries, vehicles and hazardous gases created in agriculture fields [5, 9].

Discovery of forest fire: Flue gases monitoring and monitoring of preventive fire conditions for the identification of warning areas [10].

Protection against avalanches and landslides: Monitoring of the water stored in the soil, density of the Earth and vibrations to discover harmful patterns in earth states.

Wildlife protection: Tracking calls use GSM/GPS modules to discover and trace wildlife and supply their co-ordinates through SMS.

Premature earthquake discovery: Distributed control in certain quake areas.

Monitoring oceans and coasts: Using a variety of sensors combined in aircraft, ships, satellites etc for maritime security, fishing vessel tracing and unsafe oil supplies etc.

Weather station networks: Research of meteorological conditions in agricultural land to predict the formation of ice, drought and air change.

1.5.7 Smart living

Water and energy consumption: Monitoring energy and water use to get advice on how to save costs and resources.

Smart shopping system: Get advice on where to sell based on consumer preferences, buying behavior, the existence of allergies, or expiration dates.

Remote control devices: Remotely turn on and off devices to prevent accidents and for energy saving.

Smart home products: Transparent LCD display refrigerator that shows what is inside, expired food details, ingredients for a well-stocked kitchen and all the data obtainable through the app on the smartphone [11]. Washing machines permit one to control the laundry from far away and work routinely when electricity prices are very low. Smart cooking apps monitor the automatic cleaning function of the oven and permitting adjustable temperature control from a distance.

Meteorological station: Shows conditions of the outside weather, for example, humidity, heat, atmospheric pressure, air velocity and rainfall using meters capable of transmitting information over long distances.

Regular checking of safety procedures and standards: Baby alarm, an optical tool used to record images, and house alarm schemes that are making human beings feeling safer in their everyday lives at home.

Gas detector: Real-time data concerning gas consumption and the state of gas piping can present by linking local gas meters to the internet protocol (IP) network. Concerning monitoring and assessing water quality, the result could be a diminution in labour and repair prices, enhanced precision and meter readings price reduction, and perhaps gas usage diminution.

1.5.8 Smart health

Activity monitors as support for older persons' physical activity: Wireless body area network measures movement, critical signals, blurred vision and the cellular unit, gathering, displaying and storing activity information.

Falling-detection: Help for the elderly or disabled who live independently.

Pharmacy refrigerators: The conditions of the regulation within cold storage for storing medicines, vaccines and organic components.

Patient monitoring: Surveillance of patient health status within hospitals and nursing homes.

Personal care of sports people: Vital sign monitoring in high-performance areas and camps. Fitness and health manufacture for these reasons are available, that calculate fitness, steps, weight, blood pressure, and other details.

Managing chronic illness: Patient surveillance programs with full patient details can be obtainable for monitoring chronic illness patients remotely. Admission to a reduced medical facility, low price, and temporary hospital stay can be just a few of the advantages.

Hand hygiene approach: Monitoring scheme by using RFID tags for wristbands with the integration of Bluetooth LE tags at the patient's hand hygiene control, where vibration alerts are transmitted to notify during handwashing. The entire information gathered generates statistics that can utilize tracking patient morbidity in specific health staff [8].

Ultraviolet light: Measuring UV sunlight to alert humans not to be exposed at specific times.

Oral care: A Bluetooth-connected dental brush with an app on the smartphone examines the task of brushing teeth and provides details on the smartphone to obtain confidential information or to show statistics to the dental surgeon.

Sleep control: IoT devices situated across the bed sense usual movements, such as breathing and heartbeat and huge movements caused by tossing and turning at night when asleep, presenting information obtainable via the smartphone app.

1.5.9 Smart water monitoring and smart food

Water Leaks: Discovery of water availability in outside tanks and pressure differences in pipelines.

Quality of water: Analysis of the appropriateness of water in natural flowing watercourses and oceans for all of the animal life present in a particular region or time and the appropriateness for potable usage.

Flooding: Monitoring the variability of flow rates of rivers, reservoirs and dams.

Control the supply chain: Monitoring storage conditions during supply chain activities and manufacture tracing for tracking reasons.

Water management: Real-time data concerning water condition and water usage can gather by linking a water meter to the IP network [12].

Enhancement of wine excellence: Monitoring water stored in the soil and trunk width in vineyards to regulate sugar levels in grapes and health of grapevine.

Grounds where the game of golf is played (golf course): Selected irrigation in arid areas to decrease the essential green-water assets.

Greenhouses: Regulate microclimatic level to increase vegetable and fruit manufacture and excellence.

In-field water quality monitoring: Decreasing food spoilage with excellent tracking, statistical management, continuous data acquisition, and crop field management, with excellent management of fertilization, irrigation and electricity.

1.5.10 Smart city

City noise mapping: Monitoring noise in the concentric zone, including bar areas in real-time.

Construction health: Vibration and conditions of materials monitoring in statues, bridges, monuments and popular buildings [8].

Traffic jam: Pedestrian and vehicle level monitoring to enhance walking and driving paths.

Safer cities: Video surveillance system, public address sound systems and fire prevention and control systems.

Intelligent lighting: Smart and weather adaptive lights in raised sources of light on the edge of a road.

IoT applications differ, and IoT applications work for various consumers. Various categories of consumers have various driving requirements. From an IoT point of view, there are three essential consumer categorizations:

- individual citizens;
- groups of citizens (citizens of a nation, state and city);
- companies.

Examples of IoT applications required by individual citizens are such that:

- Increasing their security or the security of members of their family—for instance, remote control for a security alarm system, or activity recognition for older people;
- Facilitating easy-to-perform tasks—for instance: home inventory management reminder.

1.6 Summary

This chapter describes an overview, characteristics, advantages, disadvantages, common uses, security, trust, privacy and functional view of IoT. Furthermore, we propose application areas of IoT in detail. IoT can promote a functional variety of industrial appliances like logistics, manufacturing, food business and services. Novel standards, novel trade, competition, and the need to transport nonstop goods are challenges new businesses face nowadays. As a result, a lot of companies rely on Industrial Internet of Things (IIoT), which refers to any performance executed by businesses to model, supervise and enhance their business processes during insights gathered from thousands of linked machines to assist them in enhancing economical profit. Therefore, the next chapter discusses IIoT in detail.

References

[1] Nia A M and Jha N K 2017 A comprehensive study of the security of Internet-of-Things *IEEE Trans. Emerging Top. Comput.* **5** 586–602

[2] Daud M, Rasiah R and George M 2018 Denial of service: (DoS) impact on sensors *4th Int. Conf. on Info. Management (ICIM)*

[3] Yang Y, Liu X and Deng R H 2018 Lightweight break-glass access control system for healthcare Internet-of-Things *IEEE Trans. on Industrial Informatics* **14** 3610–7

[4] Yang Y, Wu L, Yin G, Li L and Zhao H 2017 A survey on security and privacy issues in internet-of-things *IEEE Internet Things J.* **4** 1250–8

[5] Jamal H, Huzaifa M and Sodunke M A 2019 Smart heat stress and toxic gases monitoring instrument with a developed graphical user interface using IoT *Int. Conf. on Electrical, Commun., and Computer Engineering (ICECCE)*

[6] Kodali R K and Rajanarayanan S C 2019 IoT based indoor air quality monitoring system *Int. Conf. on Wireless Commun. Signal Processing and Networking (WiSPNET)*

[7] Barman B K, Yadav S N and Kumar S 2018 IOT based smart energy meter for efficient energy utilization in smart grid *2nd Int. Conf. on Power, Energy and Environment: Towards Smart Technology (ICEPE)*

[8] Wu F, Wu T and Yuce M R 2019 Design and implementation of a wearable sensor network system for IoT-connected safety and health application *IEEE 5th World Forum on the Internet of Things (WF-IoT)*

[9] Muthukumar S, Sherine Mary W and Jayanthi S 2018 IoT based air pollution monitoring and control system *Int. Conf. on Inventive Res. in Comput. Appl. (ICIRCA)*

[10] Prabha B 2019 An IoT based efficient fire supervision monitoring and alerting system *Third Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*

[11] Agarwal K, Agarwal A and Misra G 2019 Review and performance analysis on wireless smart home and home automation using IoT *Third Int. Conf. on I-SMAC*

[12] Rajurkar C, Prabaharan S R S and Muthulakshmi S 2017 IoT based water management *IEEE Int. Conf. on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)*

View publication stats