Archives of Computational Methods in Engineering
https://doi.org/10.1007/s11831-021-09622-6

REVIEW ARTICLE

A Review and State of Art of Internet of Things (IoT)

Asif Ali Laghari[1,5] · Kaishan Wu[1,2] · Rashid Ali Laghari[3] · Mureed Ali[4] · Abdullah Ayub Khan[5]

Received: 3 December 2020 / Accepted: 7 June 2021

Abstract
The Internet of Things (IoT) is basically like a system for connecting computer devices, mechanical and digital machines, objects, or individuals provided with the unique system (UIDs) and without transfer to transmit data over an ability human-to-human or computer-to-human relation. Another thing on the internet is that the items in the IoT are like a connected manner with humans and computers to which internet protocol addresses can be assigned and which can transfer data over the network or another man-made object. In this paper, we describe the utilization of IoT in the cloud, fog, IoT technologies with applications and security. Specifically, we provide IoT architecture for design and development with sensors in 6G. Finally, we discuss the current research, solutions, and present open issues of future research in IoT.

1 Introduction

The Internet of Things (IoT) is becoming a step towards the revolution in the modern-day world and a milestone achieved in the field of artificial intelligence [1]. The IoT can be demonstrated by a short and simple example from our daily lives. An example of a Television is a display of IoT [2]. We can change the channel stream by sitting at a point without even touching the T.V with the help of a remote. The concept of IoT is the same; we can remotely control almost every electrical appliance in our surroundings [3]. IoT is a great technology that influences us, judging from the way we react to the behavior of ourselves in our daily lives [4]. From electrical home appliances (like fridge AC) and remote-controlled appliances (like TV) to vehicles providing the shortest and safest route to us [5]. All can be controlled by using smartphones including our smartwatch.

IoT is a large network comprising of devices connected to it as given in Fig. 1 [6]. The devices connected gather data and share how they are being operated and perform assigned tasks [7]. It is all thanks to sensors. They are embedded in our mobile phones and various other electrical appliances and signal-based devices that will be connected to the network of IoT.

An IoT ecosystem involves web-enabled smart devices that use incorporated systems, such as processors, sensors, and communication hardware, to assemble, send, and act on the data they obtain [8]. IoT devices reveal the sensor data they assemble by involving an IoT entry or other edge device where the data is sent to the cloud for analysis or on-premises analysis. Now And Then these devices communicate with other connected devices and act on the information they obtain from each other. Devices do most of the work without human intervention, although people can interact with devices, for example, to configure, instruct, or access data [9]. The connectivity, networking, and communication protocols used with these web-enabled devices are highly dependent on the specific IoT (internet of things) applications implemented. IoT is the one that can also be able to machine learning, which is called

✉ Kaishan Wu
wu@szu.edu.cn

Asif Ali Laghari
asifalilaghari@gmail.com

Rashid Ali Laghari
rashidali@stu.hit.edu.cn

Mureed Ali
mureedali6@gmail.com

Abdullah Ayub Khan
abdullah.khan00763@gmail.com

1 College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China

2 HKUST Fok Ying Tung Research Institute, Guangzhou, China

3 School of Mechatronics, Harbin Institute of Technology, Harbin, China

4 QUEST Nawabshah, Nawabshah, Pakistan

5 Department of Computer Science, Sindh Madressatul Islam University, Karachi, Pakistan

Published online: 14 July 2021

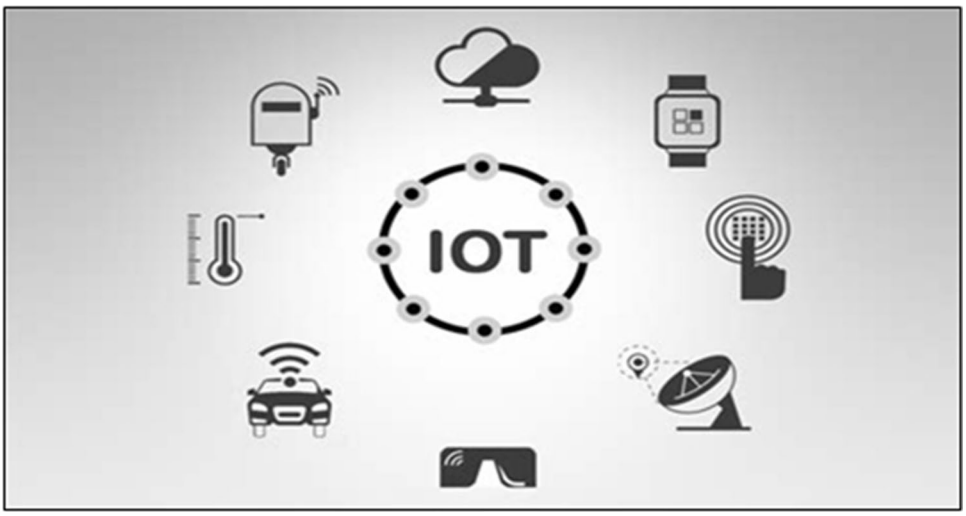

Fig. 1 IoT network connected with of devices

artificial intelligence that can help to make data more convenient processes and much more dynamic [10, 11].

The IoT consists of connected systems, sensors, automobiles antenna, and much more [12]. Since IoT creates and analyzes large amounts of data, it is a major engine of big data analytics projects [13]. In particular, it can bring large amounts of data in real-time [14]. Through various IoT devices, it is possible to display the performance of all employees, as well as advance operations at all locations. The example of IoT data collection to data processing is given in Fig. 2 [15].

The paper will address the topic of IoT, the state of the art of IoT, and how IoT is used for fog, in 6G, and cloud computing. It surveys IoT architecture and sensors used in development and security together with their potential applications, such as system tuning and diagnosis. Limitations of previous work and challenges of future work are also discussed. Further, we identify and discuss a set of open issues yet to be addressed, for accurate implementation and operating of IoT for cloud, fog, and 6G networks.

This paper is based on the IoT survey and review in different areas and is divided into 10 sections. Section two is based on IoT architecture, the section is based on IoT technologies.

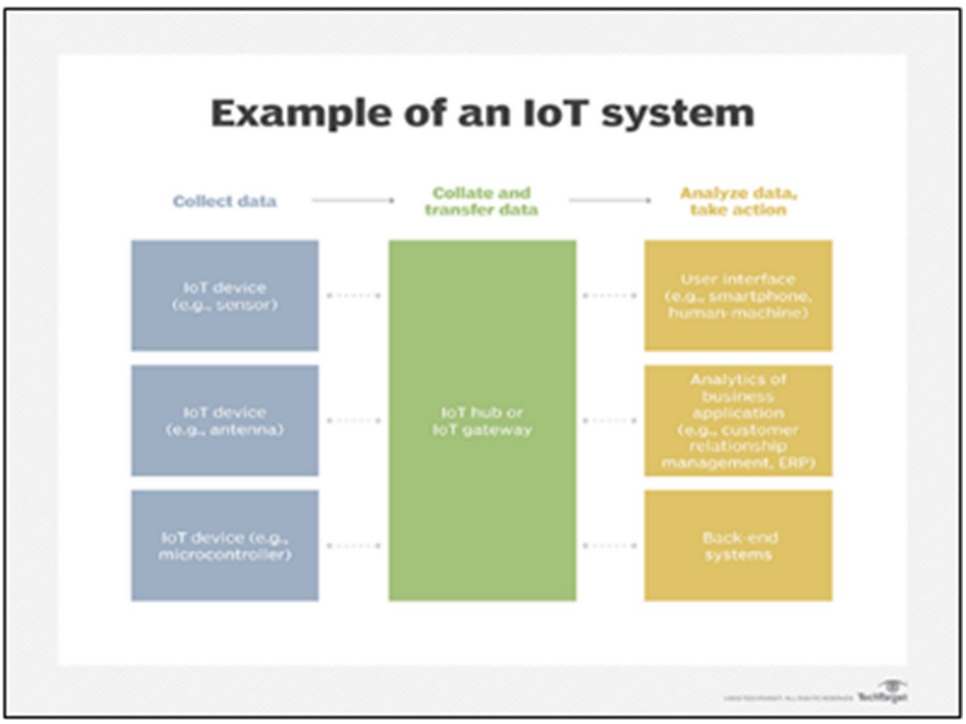

Fig. 2 IoT data collection to data processing

Similarly, sections four, five, six and seven, are based on the IoT utilization in Cloud, fog, and 6G networks respectively. Section 8 is based on IoT applications and Sect. 9 is based on IoT security and privacy. Finally, in section ten, we present the open research questions in this field.

2 IoT Architecture

Nowadays, the Internet has gotten omnipresent, has reached each side of the world, and is impacting human life in incomprehensible manners. Nonetheless, the excursion is a long way from being done. We are directly getting into a time of much progressively inescapable network where a wide variety of machines will be related to the web. We are entering a period of IoT and the term has been characterized by various creators from various perspectives. We utilize these capacities to question the condition of the item and to change its state if conceivable. In like way discourse, the IoT suggests such an existence where practically all the devices and apparatuses that we use are associated with a system. We can utilize them cooperatively to accomplish complicated assignments that require a serious extent of insight. Different structures have been proposed by different specialists; however, there is no single architecture that is standardized by any organization for IoT, which is concurred for the most part [16–18]. We discuss different sensors in this paper, which are used in the design and development of IoT architecture.

2.1 Sensors

All IoT applications need to have at least one sensor to gather information from nature [19]. Sensors are basic parts of shrewd items. One of the most significant parts of the IoT is setting mindfulness, which is absurd without sensor innovation. IoT sensors are for the most part little in size, have minimal effort, and devour less force. They are obliged by components, for example, battery limit and simplicity of sending. Schmidt and Van Laerhoven give an outline of different sorts of sensors utilized for the development of intelligent applications [20]. Different types of sensors are used in IoT applications are given in Fig. 3.

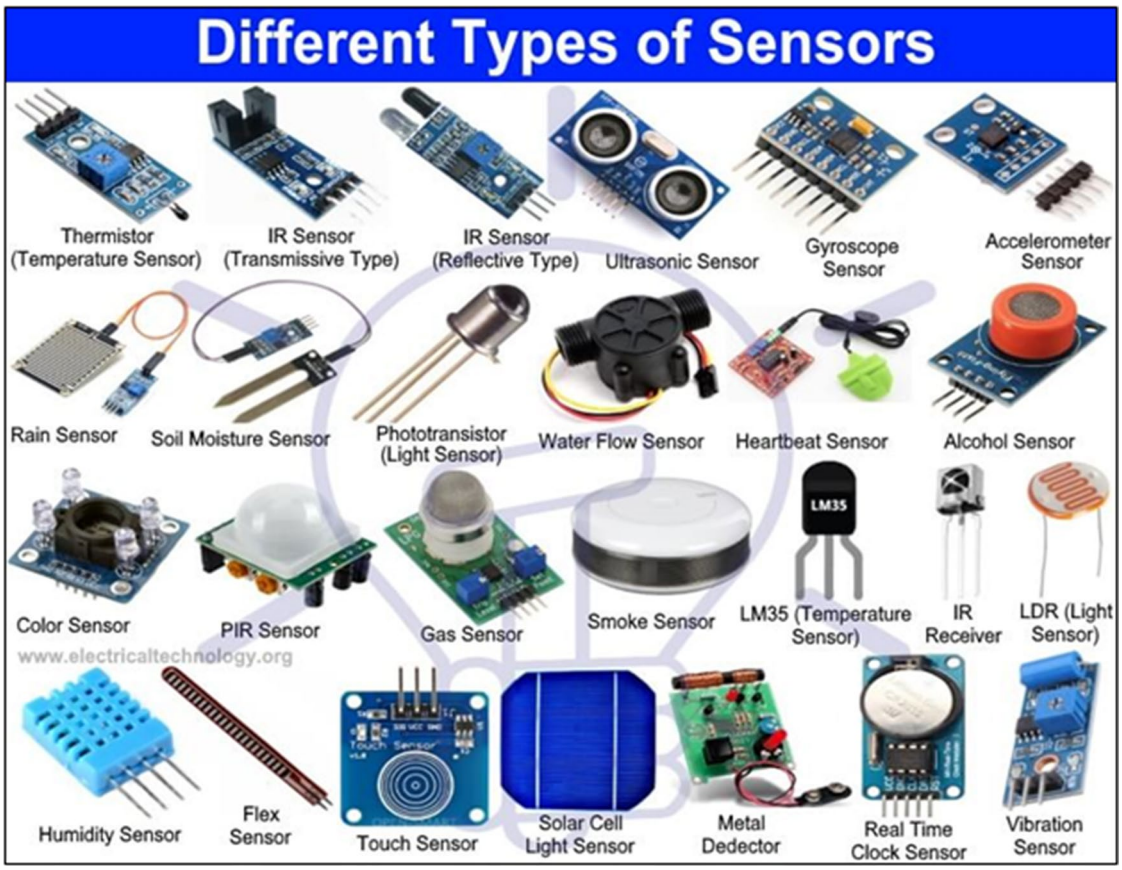

Fig. 3 IoT sensors

2.2 Mobiles Sensors

Above all else, let us take a look at the cell phone, which is universal and has numerous kinds of sensors installed in it. In explicit, the cell phone is an extremely convenient and easy-to-use device that has a large group of inherent correspondence and information preparing highlights. With the expanding prominence of cell phones among individuals, scientists are indicating interest in building intelligent IoT arrangements utilizing cell phones due to the installed sensors [21]. Some extra sensors can likewise be utilized relying on the prerequisites. Applications can be based on the cell phone that utilizes sensor information to deliver significant outcomes [22].

2.3 Neural Sensors

Nowadays, it is far plausible to recognize neural symptoms in the mind, surmise the situation of the cerebrum, and educate it for better consideration and center interest [23]. It is called neuro remarks the innovation applied for perusing mind alerts is called Electroencephalography (EEG) or a cerebrum PC interface [24]. The neurons inner the thoughts impart electronically and make an electric field, which can be estimated from outside concerning frequencies. Mind waves can be organized into the delta, theta, gamma, beta, and alpha waves counting on the recurrence.

2.4 Actuator

There are certain instances of actuators that are utilized on the IoT [25, 26]. An actuator is a device, which can impact an adjustment in the earth by changing over electrical vitality hooked on a certain type of valuable vitality. A few models are cooling or heating components, lights, speakers, shows, and engines. The actuators, which instigate movement, can be arranged into three classes, to be specific, electrical, pressure-driven, and pneumatic actuators relying upon their activity. Pressure-driven actuators encourage mechanical movement utilizing liquid or water-powered force. Pneumatic actuators utilize the weight of packed air, and electrical ones utilize electrical vitality.

2.5 Low Energy Bluetooth

Low Energy Bluetooth (LEB), otherwise called "Intelligent Bluetooth," was created by the Bluetooth Particular vested party [27]. It has a moderately short-range and devours low vitality when contrasted with contending conventions. The LEB convention stack is like the stack utilized in great Bluetooth innovation [28]. It has two sections: controller host. The physical and connection layer is executed in the controller. The controller is regularly a SOC (Framework on Chip) with a radio. The functionalities of higher layers are remembered for the host. BLE is not perfect with great Bluetooth. Let us take a look at the contrasts between great Bluetooth and LEB.

The fundamental distinction is that LEB does not boost information flowing. Rather, it reinforces the fast exchange of little bundles of information (parcel size is little) with an information pace of one Mbps.

There are two sorts of devices in LEB: ace and slave the ace goes about as a focal device that can interface with different slaves. Let us consider an IoT situation where a telephone or PC fills in as the ace and cell phones, for example, an indoor regulator, wellness tracker, intelligent, or any checking device go An as slaves. In such cases, slaves ought to be very force productive. Thusly, to spare vitality, slaves are of course in rest mode and wake up intermittently to get parcels from the ace.

In exemplary Bluetooth, the association is constant regardless of whether no information Move goes on. Furthermore, it underpins 79 information channels (1 MHz channel transmission capacity) and an information pace of one million images/s, though, LEB bolsters forty channels with two MHz channel transfer speed (twofold of exemplary Bluetooth) and 1 million images/s information rate. BLE boosts low obligation cycle necessities as its parcel size is little and the time taken to transmit the littlest bundle is as little as 80 s. The LEB convention stack underpins IP based correspondence too. An investigation led with the aid of Siekkinen et al. recorded the number of bytes moved in line with Joule to expose that BLE expends far less vitality when contrasted with contending conventions, for example, Zigbee. The vitality effectiveness of LEB is 2.5 occasions better than Zigbee [29].

3 Technologies for IoT

It is a difficult task to outline the technology that forms the future-based technology that controls the sheer number of inventions and discoveries surrounding us. However, we can illustrate it by dividing the great stack into four different bases that are involved in the making of IoT given below and also represented in Fig. 4 [30, 31].

- System hardware
- Software device
- Communication route
- Platform

3.1 System Hardwar

These form the physical body of the system; they are the components referred to as “things” in the title of IoT [32].

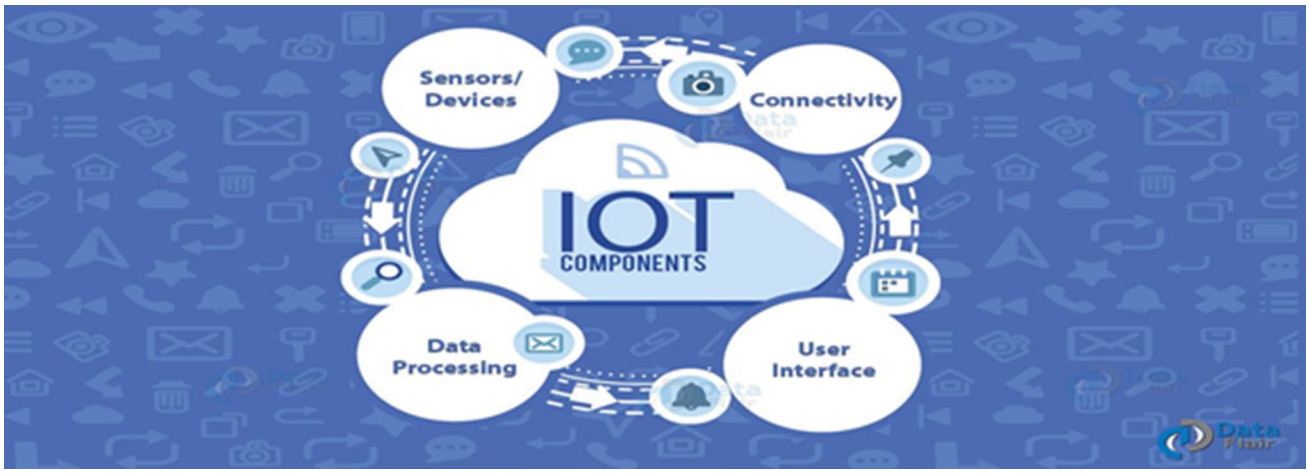

Fig. 4 IoT infrastructure and devices

They act as the doorway between reality and the digital world. They are observed in many forms, like a sensor in a phone or an automatic driving car [33]. Any physical wired device that may become 'smart' by adding a chip or a sensor or a board for controlling it through signals is called IoT hardware.

These devices are greatly used for gathering data about their respective fields. Many sensors and microprocessors are plotted inside the devices to make it smart but, a small problem rises that may be countered later in the future, i.e. the high amount of cost of purchase, a large amount of money is required for purchasing [34, 35]. Another problem is the compatibility of the device; many devices are not compatible with the newly invented sensors that may be reduced over time [36, 37].

3.2 Software Device

The second step towards the construction of IoT is the software device [38]. The word 'smart' may be used as it works as the brain of the IoT system [39]. The implementation of data and cloud communication falls into this department. It is responsible for device integration and system data collection, and analysis of data within the cloud performed by the IoT software. It also enables the user to interact with the system by converting the data into application-level capable to be visualized by the user. The data received from devices is in the analog form it is converted into digital streams by DAS (data acquisition system) by performing all logical analytical and theoretical operations. After processing, the data before entering the data center, the same process of operations is repeated by the IT edge to make it more exact and informative.

3.3 Communication Route

It is the third base of the IoT system [40]. After completing the set-up for the hardware system and device software and making it ready, there comes the communication stage, which is responsible for providing the route for transmission of the newly generated smart hardware devices. The communication system is based on hardware and software systems but, its importance should not be neglected, as it has importance in the IoT system [41]. First, we have to decide the route for transmission of data; we have several choices available in the market. These choices may include Wi-Fi LAN Bluetooth or satellite controlling. Each of them is suitable for transmission if they have their respective hardware and software installed. Every communication chip has its separate configuration and cloud structure, and not only will it decide the way of sending but also how the devices are managed and communicate. The importance of communication in IoT may be explained by an example of a ladder with no steps [42].

3.4 Platform

This is the fourth and final of the IoT system. By making the correct choice of hardware and selecting the efficient software type that makes the data compatible and transforms it into information and by selecting the proper communication channel our work is almost complete [43, 44]. The fourth and final step, which is the platform, where all the above gathered and processed data is stored. From here the data is presented to the user in a user-friendly form. In this section, data is categorized and divided according to its purpose. The platform acts as a cupboard with different shelves for storing different clothes similarly the platforms also work in the

same way. The data is labeled and stored on different shelves [45]. Through this, the user could pick the exact information. There are many companies in the market providing platforms depending upon the characteristics and structure of the platform [46]. The choices may vary on the cost and requirement. There are many companies offering platforms, which may be either installed on the device using extra storage device or use cloud storage. An example can be taken as azure or cybersecurity works.

IoT has many stages that repeat one after another. The first step is the gathering of data that is done through sensors or in the above words "device". The second step is the transfer of data to the cloud, which is done through many mediums like Wi-Fi etc. once the data is collected we move on to the next step, which is the processing of this data through different checking software and valuable information is obtained. The last step is the user interface. The user e.g. gets notified through emails and alarm alerts [47]. In many cases, sometimes the actions are performed without the interference of the user. The system at some point is capable of making its own decisions. It can be explained by taking the example of an uninvited person or an intruder being sensed in the zone that may make the alarm or security system go off. Not only making the owner but also instantly calling the police or contacting the concerned security department. That is why the IoT system is becoming a 5star module nowadays and looking at the high chart ratings there is no stopping it [48].

4 Cloud IoT

Google Cloud IoT is a finished arrangement of devices to associate, procedure, store, and break down information both at the edge and in the cloud [49]. The stage comprises versatile, completely oversaw cloud benefits; an incorporated programming stack for edge/on-premises figuring with AI capacities for all your IoT needs [50, 51]. The Cloud IoT scenario is shown in Fig. 5 [52].

IoT has progressed with the more prominent age of data. Web of Things Cloud Service makes over the best correspondence between cheap sensors within the IoT, which suggests altogether more prominent accessibility; billions of related devices and machines will sometimes recently long connect human-clients [53].

4.1 IoT Cloud (Salesforce IoT Cloud)

IoT cloud is organized from Salesforce.com that is planning to store and strategy the IoT data [54]. The IoT Cloud is controlled by Thunder, which Salesforce.com portrays as a "hugely versatile consistent event planning engine [55]." The stage is worked to require within the tremendous volumes of data created by contraptions, sensors, sites, applications,

Fig. 5 Cloud IoT scenario

clients, and assistants and start exercises for progressing responses. For instance, wind turbines might adjust their conduct subordinate to current climate data; airplane travelers whose comparing flights are conceded or dropped might be rebooked sometime recently the planes they are on have landed.

In another unique situation, IoT Cloud can furnish business clients with a much significantly completer and more incorporated viewpoint on clients, without requiring specialized skill or the administrations of an information investigator [56]. The stage can take in billions of events a day, and clients can assemble choices that decide events to take after upon and what moves to create. IoT cloud is data setup and thing skeptic; surrender connectors allow correspondence with Salesforce fogs or outsider organizations.

Salesforce.com is a San Francisco-based client relationship with the board (CRM) and social endeavor programming as-an organization (SaaS) supplier [57]. The organization moved IoT Cloud within the fall of 2015, at its annually Dreamforce client gathering.

4.2 Salesforce Outlines What to Expect from IoT Cloud

SAN FRANCISCO—At Dreamforce 2015, Salesforce prepared for the approaching Internet of Things (IoT) upheaval by discharging the IoT Cloud [58]. Based on the advancement stage known as Thunder, the IoT Cloud will gather and store information that originates from interconnected devices, yet also make that data promptly accessible to improve client experience, said Dylan Steele, ranking executive of item showcasing for the IoT Cloud at Salesforce [59].

One of the qualities of the IoT Cloud, Steele said at the gathering, is making the information assortment process simpler for business clients. Less-specialized clients no

longer need to depend on information experts to capitalize on the information. The IoT Cloud includes an occasion preparing motor that ingests billions of occasions for each day, Steele stated, and the stage permits clients to assemble decides on the head of that information to recognize explicit occasions to follow up on. The IoT Cloud has yield connectors appended to it that can associate with some other Salesforce cloud or outsider framework an organization picks.

Steele likewise talked about the IoT Cloud's security structures, saying the stage is based on a similar innovation supporting other Salesforce items and conveys their security measures with it. Steele said the IoT Cloud is information arrangement and devices skeptic, so it can work with information originating from different devices and send the information to any framework, for example, its Sales and Service Clouds or outsider frameworks.

4.3 IoT and Cloud Computing for Future Internet

The inquiry anyway remains by what means will the devices stay interconnected all through. The appropriate response lies in the network gave by the web of things cloud administration. More noteworthy utilization of the IoT in the cloud has gone about as an impetus for the turn of events and sending of adaptable IoT applications and strategies of achievement. Cloud/fog computing and IoT have become two firmly associated upcoming web revolutions with one giving the other a step to advance [60]. There are various advantages, which the intermingling of IoT and Cloud registering has determined.

4.4 Providing Infrastructure

IoT within the cloud offers open cloud organizations that can without much extending help the IoT domain, by giving untouchable get to the establishment. Hence, the joining can offer assistance IoT data or computational portions working over IoT devices [61].

Expanded Scalability IoT devices require an extraordinary deal of capacity to share information for important purposes. IoT within the cloud, comparable to the StoneFly Cloud Interface to Microsoft Azure can deliver clients more conspicuous space, which can increase agreeing to the client's request and helping with settling the capacity needs of clients.

Expanded Performance A lot of data made by IoT devices needs over-the-top execution to collaborate and interface with each other [62]. IoT within the cloud gives accessibility, which is imperative to share information between the devices and make noteworthiness from it at a fast pace.

Pay-More Only as Costs Arises Cloud computing frameworks help IoT to offer significance to the more prominent measure of information created. Clients have no concern about purchasing more prominent or less stockpiling. They can without much-extended scale the capacity as the data made increases and pay for the degree of capacity, they use with cloud computing.

4.5 Is the Cloud fascinating for IoT?

So far, we have exclusively been examining the upsides of misusing the cloud for IoT. We should in a matter of seconds.

- Decreased costs, each immediate and foundation
- Pay-varying for capacity/registering
- High framework quantifiability and availability
- Increased lifetime of controlled sensors/devices
- Ability to mix monstrous measures of information
- Anything with an online affiliation will become "shrewd"

In any case, there square measure genuine issues with cloud utilization:

- *Data ownership* After you store data during an organization's cloud administration, does one own {the data the information} or will the cloud supplier? This could be hugely essential for IoT applications including individual information like consideration or reasonable homes [63].
- *Potential crashes* On the off chance that the affiliation is hindered or the cloud administration itself crashes, the IoT application will not work [64]. Short inoperability will not be a huge arrangement sure IoT applications, as reasonable farming, anyway it might be decimating for other people. You need not bother with applications including wellbeing or security unmitigated for even numerous seconds, in addition to numerous hours.
- *Latency* It requires some investment for data to be sent to the cloud and orders to return to the devices [65]. Ensure IoT applications, these milliseconds will be crucial like in wellbeing and security a not too bad model is Self-sufficient Vehicles. If an accident is looming, you do not have to claim to go-to for the car to address the cloud before deciding to turn out of the methods.

5 Fog IoT

"Fog computing is a dispersed computing organization or procedure in which computing resources are located among a data source and a cloud or other files center [66, 67]." Cisco introduced the fog computing term. Fog computing is the one nearer to deal with the IoT [68]. Fog computing also known as a network of fogs or clouds is a decentralized place at the most logical and efficient point between data sources and the cloud [69]. Fog computing is a reorganized IT structure where records, processing, storage, and tenders

are halfway among the data foundation and the cloud. Alike edge computing, fog computing provides the benefits and capabilities of the cloud somewhere data is generated and processed. Many people use the terms "fog computing" and "boundary computing" interchangeably, as they imply that intelligence and processing are closer to the place where the data is generated. This is often done to increase efficiency, although it can also be used to ensure safety and compliance.

Fog used where data should be analyzed with a fraction of the second and huge quantity of policies. The strategies are located at a very environmental distance, and device equipment is subject to extreme conditions. Fog nodes provide transitory storage, computing capability to develop the records before it is sent to the cloud, and gross fast judgments. The network connectivity is to attach with IoT devices, extra fog nodes, cloud, routers, surrounded servers, alterations, and video shadowing cameras, etc. [70]. Deployable somewhere exclusive the network and every fog node take its cumulative fog node [71].

Fog processing is based on three types of data such as very time-sensitive data, less time-sensitive data, and not time-sensitive data. Fog nodes are always works rendering to folks kind of records whatever they obtain. An IoT presentation would be mounted to a piece of fog bulges. The nearby fog node ingests the statistics from the policies.

- *Very time-sensitive data* Data to be considered inside a split second. Investigate at the adjacent node itself. Conducts the judgment or stroke to the campaigns, conducts, and supplies the summary to the cloud for upcoming inquiry [72].
- *Less time-sensitive data* Data that becomes investigated after minutes or seconds. This data is referred to as the comprehensive node for inquiry. Later exploration, the combined node leads the resolution or act to the device over the bordering node. The collective node guides the summary to the cloud for storage and upcoming analysis.
- *Non-time-sensitive data* The data which be able to pause for weeks, days, and hours. Referred to the cloud for imminent storage and breakdown and a summary of the fog nodes can measure less time-sensitive data.

A fog computing environment can take many devices and purposes dependent on its presentation. It might contain processing accesses that receive data from data causes or multiple gathering endpoints, such as routers and switches, which connect resources to the network.

In the procedure of shifting data through fog computing construction in an IoT environment, the automated controller reads signals from IoT devices [73]. The controller (reader) launches the system program necessary for the automation of IoT devices. Program the data governor system platform drives to a customary OPC core attendant or other gateway procedures. This information is translated into an agreement that the Internet service provider can understand, such as MQTT or HTTP (S). After the conversion, the data will be updated to be sent to the cloud or IoT gateway. These endpoints collect complete information for additional (additional) details or provide data to the cloud for the general public. The advantages and disadvantages of Fog IoT are given in Table 1.

5.1 Applications of Fog

Real-time health analysis:

- Patients with continuing sickness can be observed in real-time.
- Knock patients.
- Analyze the data in real-time.
- During emergency, warn the corresponding doctors directly.

Intelligence power proficient system:

- Power efficient
- Intelligences feature power construction reports every day.
- Propose economic power custom idea.

Real-time rail monitoring:

- Fog nodes can be arranged to railway paths.
- Real-time checking of the track state.
- For high-speed trains, referring the data in the cloud aimed at analysis is incompetent.
- For nodes offer firm data analysis.

Pipeline optimization:

- Requires real-time monitoring of heaviness, flow, and compressor.
- Terabytes of statistics are created.
- Sending all these records to the cloud for analysis and storage is not effective.
- Network latency is not suitable.
- Fog stays an explanation.

Analysis of wind turbines and real-time turbines:

- Wind direction and speed analysis can increase output.
- Data can be monitored in real-time.

5.2 Challenges

Power consumption:

Table 1 Advantages and disadvantages of Fog IoT

Advantages	Disadvantages
1. Decreases unwanted mishaps: Latency will be condensed throughout result creating Speedy result construction	1. Existing data protection mechanisms, such as encryption, could not secure the data from intruders
2. Superior privacy: Every productiveness can analyze their information locally Store personal data in their native servers Send only those data which can be collected to the cloud	2. It does not check whether the user has been authorized or not
3. Business agility: Fog application can be easily developed according to tools available Can be deployed anywhere we need Can be programmed according to the consumer's requirement	3. The security of cloud computing is not focused on ways to protect data from unauthorized access
4. Support mobility: Nodes are able to be mobile Nodes can be joint and leave the network at any time	4. No one is identified when the attack occurs Identifying the attacking user is difficult
5. Deployable in remote places: Can be deployed in remote places Can be subjected to harsh environmental conditions Undersea, railway tracks, vehicles, factory floor, etc	5. We cannot determine which file was cracked Increased connections mean increased risks
6. Better data management: Can work with low bandwidth Data can be analyzed locally Decrease the hazard of latency	6. Sometimes the whole concept of vague computing can seem complicated and confusing

- Fog uses additional nodes.
- Higher power consumption than a centralized cloud.

ϖ Data security:

- Data producing nodes are circulated.
- Providing substantiation and agreement systems for all nodes is not an informal task.

ϖ Reliability:

- It's hard to maintain the integrity and find millions of characters easily.
- Node corruption does not affect the website.

ϖ Fault tolerance:

- A node failure should be fixed immediately.
- Individual failure should not affect the entire scenario.

ϖ Real-time analysis:

- Real-time analysis is a primary need for minimizing latency.
- Dynamic analysis and decision making reduces the hazard and improves results.
- It is not easy to track a large number of nodes.

ϖ Programming architecture:

- Fog node can be done by mobile.
- Nodes can be connected to or disconnected from the network as needed.
- Many data processing structures are static.
- In such a structure, adequate scalability and flexibility cannot be provided.

Fog is an ideal partner for cloud and IoT [74]. The IoT resolves the major problems facing the cloud when managing IoT data [75]. Benefits range from one person to large companies provides analysis and monitoring in real time.

6 IoT with 6G

Nowadays, the IoT emerges as technology comes with the great capability of smart controlling, various physical devices around the world connected to the internet to share and receive data. Dong et al. defined IoT as "more than a buzzword; a system that provides a new way to interact with technology and behave of a human being [76]. Connecting physical devices that until being connected and control smartly" [76]. The technology is embedded with digital software, sensors, and other computing technologies for exchanging data with distinct devices wirelessly over the internet. On the other side, technological advancement and evolution in computing hardware and wireless communication, such as generation 6 (6G) [77, 78] make it possible to control every physical device, for example, as small as

a ubiquitous chip to as huge as the unmanned aerial vehicle. These technologies fulfill the massive need of the world population for providing fast as well as secure communication with the promising solution of wireless energy transfer enabling technology, 6G also handles higher frequency and wider bandwidth [79, 80]. Highlighted features of IoT with 6G are as follows [81]:

- Allow to build a technological business model;
- Automate manufacturing as well as business processes;
- Collect effortless source of revenue;
- Provide customer-centric services;
- Network slices capability;
- Facilitate a distributed network application for cloud optimization;
- Automatic life-cycle management for network application;
- Provide advance modulation scheme;
- Evolution of 6G, enhance bit rate, high reliability, low latency, high spectral and energy efficiency compares to 5G [82];
- An intelligent network also provides green communication.

6.1 IoT Architecture with 6G

IoT starts with connecting, technology:

6.1.1 Advantages

- *Strong Communication* IoT with 6G encourage Machine-to-Machine (M2M) communication, able to connect physical devices, complete availability of transparency with reducing inefficiencies and high quality [83].
- *Powerful Automation and Control* All the physical devices are connected and digitally sharing data resources using wireless infrastructure, a huge amount of powerful control and automation system handle the complete scenario. Without human intervention, the machine can communicate with others leading to faster and more on-the-spot output [84].
- *Information Discovery and Monitoring System* From a business point of view, having more information help for making better decisions. Monitoring the exact quality and quantity of supplies, able to provide more information that could not be collected previously, monitor and improve expiration of products in the future.
- *Reduce Cost and Time* Fundamentally, IoT proves very useful for people in their daily life, makes electronic appliances smart that efficiently communicate with each other, saves cost, time, and energy.
- *More Speed and Adopting New Standards* IoT enables us to complete complex tasks faster along with efficiently [85], automate daily routine tasks easily, for example, smart offices. The intelligent device automatically updates the system according to the new standards.

7 IoT Applications

IoT applications try to make major shifts in our lifestyles. With more up to date wireless setups, powerful sensors, and improving computing capacities, the IoT could be the upcoming next big thing in our modern lives and will continue to make our life easier [86]. With the help, IoT tech giants companies are trying and already are making our lives connected. As per Gartner's research, by 2020 connected devices including all the technologies will reach 20.6 billion, which is tremendous [87].

These devices will overcome and bridge the gap between the physical and digital world to improve the way of living, society, and corporations. With IoT making up for Smart houses is a much-anticipated element, with organizations now competing with their smart devices and appliances [88]. Wearable tech is another component shifting rapidly on the web. With the releases of apple wearable tech and Samsung gear and similar wearable tech from other companies recently and more devices coming, these devices are going to keep us connected with the interconnected globe [89]. Nevertheless, the hype nowadays for IoT is very big. It appears that every other day a firm launches its new IoT-enabled item.

Following are the top IoT applications as ranked on the internet by popularity from Google searches or people talking about it on a different forum such as Twitter, Facebook, Reddit, etc.

7.1 Smart Urban Cities

Smart cities are another great use of IoT [90]. Automated transportation, urban security, smart energy managing systems, smart surveillance, water supplying, and environmental tracking, are some samples of IoT uses for smart urban cities [91]. It is known for the fact that many Smart cities solutions promise to upgrade the lifestyle of individuals living in urban communities nowadays. IoT solutions in the field of Smart cities solve traffic jam issues and reduce noise pollution and help make urban areas more secure.

7.2 Connected Automobile

Connected Automobile is also coming up [92]. In a few years, we would see IoT implementations in budget sector cars too. In the past, this technology was only focused to make vehicles internally optimized, but nowadays the attention to make the in-car experience great with the help of IoT

is growing too [93]. Major brands in both the tech and automobile industry such as Google, Apple, BMW, Mercedes, and Tesla are trying to bring the next big revolution in the automobile sector.

7.3 Wearables

Wearables are a very in-demand tech product in recent years [94]. It has gained its users from all walks of life like teenagers, middle-aged people, and even older people because of its simplicity to use and health benefits such as sleep tracking, heartbeat sensors, oximeter, pulse calculator to name a few. Tech giants like Google, Apple, and Samsung have invested a heavy amount of money to build such devices [95]. These devices serve the purpose of health, fitness, and entertainment. Wearable tech is full of sensors beneath it and a screen on top of it. It usually has the software of its maker, which provides the user with a great user experience.

7.4 Smart Retail

IoT can perform great in this field of Smart Retail [96]. With the help of IoT, retailers can connect with their respective customers. The smartphone will be a device, which will be mostly used for this purpose. Customers can also pay with their phones through mobile banking applications and can track their orders through the service provided by their retailer [97].

7.5 Digital Health

IoT in healthcare is growing in the last few years and will continue bigger in the upcoming years and decades [98]. IoT in the healthcare department encourages people to by using connected devices and live a healthier life. The concept of connected digital health has great potential for both the people and the firms of medicine and pharmaceutical industries, yet it has not reached the majority of people.

7.6 Smart Farming

With the number of people living on the planet and their growth is increasing day by day the demand for food is also increased. In such a scenario smart farming is one of the fastest and more importantly useful growing fields in IoT [99]. Not just it helps the farmers or agricultural organizations to grow more income, but it also helps the consumer to get the food in much cheaper and greater quality. Farmers are using IoT equipped devices for controlling the water supply for plants, getting the information of the soil's nutrients and moisture [100].

7.7 Smart Supply Chain

The supply chain is yet another field getting technological advancement like other fields. IoT helps in this field regarding the tracking and organizing of products or managing the inventory information [101]. E-commerce companies like Amazon, Aliexpress, Daraz use the Smart Supply Chain management in their warehouses to get the work done easily and more efficiently.

7.8 Industrial Internet

The industrial internet has great growth potential, many market researchers see the Industrial Internet as the IoT concept with great possibilities [102]. The main idea behind Industrial IoT is that machines are more precise than humans in communicating with the data, which can be used by companies to analyze more data in lesser time.

7.9 Smart Home System

Brilliant homes are turning out to be progressively mainstream today in light of two reasons. To begin with, the sensor and incitation advancements nearby remote sensor frameworks have a general sense created. Second, people nowadays believe advancement to address their interface in their fulfillment and security of their homes [103]. An illustration of a smart home system is given in Fig. 6.

In intensive houses, different sensors are sent, which offer smart and mechanized types of assistance to the client [104]. They help in mechanizing day-by-day assignments and help in keeping up a daily schedule for people who will in general be absent-minded. They help in vitality preservation by killing lighting and electronic devices consequently. We normally use movement sensors for this reason. Movement sensors can be moreover utilized for security also.

Smart domestic applications are extremely helpful for the old and diversely abled [105]. Their wellbeing is checked, and family members educated quickly if there should be an occurrence of crises. Floors are furnished with pressure sensors, which tune the development of a person over the intensive home and help in recognizing if an individual has tumbled down. In brilliant homes, CCTV cameras can be utilized to record occasions of intrigue. These would then be able to be utilized to include extraction to discover what is happening.

7.10 Smarts Water System

Given the predominant measure of water shortage in many parts of the world, it is critical to deal with our water assets proficiently. Subsequently, most urban areas are deciding on brilliant arrangements that location a lot of meters on

Fig. 6 Smart Home system

water gracefully lines and tempest channels. A decent reference around there is the paper by Hauber-Davidson, Idris [106]. They portray different structures for intelligent water meters. These meters can be utilized to gauge the level of water inflow and outpouring and to recognize potential holes. Deep-water metering frameworks are likewise utilized related to information from climate satellites and waterway water sensors. They can likewise assist us with anticipating flooding. Figure 7 shows the water conservation for future generation.

7.11 Smart Agriculture and Environment

Natural boundaries, for example, temperature and moistness are significant for farming creation. Sensors are utilized by ranchers in the field to quantify such boundaries, and this information can be utilized for proficient creation [107]. One application is a robotized water system indicated by climate conditions. Creation utilizing nurseries is one of the primary uses of IoT in horticulture. Natural boundaries estimated as far as temperature, soil data, and dampness are estimated progressively and sent to a server for investigation. The outcomes are then used to improve crop quality and yield. Example of smart environment with IoT is given in Fig. 8 [107].

Pesticide deposits in crop creation are identified utilizing an Acetyl cholinesterase biosensor. This information is spared and examined for removing helpful data, for example, the example size, time, area, and measure of deposits. We would thus be able to keep up with the nature of the yield. Besides, a QR code can be utilized to interestingly distinguish a container of ranch produce. Buyers can filter the QR code and check the measure of insecticides in it (through a unified database) on-line before purchasing.

Air contamination is a situation these days since it is changing the ecosystem of the earth and debasing air

Fig. 7 Smart management system with IoT

Fig. 8 Smart environment with IoT technology

quality. Vehicles motive a ton of air contamination. IoT software is proposed by Manna et al. to screen air contamination in the streets [108]. It likewise tracks cars that reason an undue degree of contamination. Electrochemical harmful gasoline sensors can likewise be utilized to quantify air contamination. Vehicles are outstanding by way of RFID labels. RFID peruses are put on the two roadsides along with the gas sensors. With this methodology, it is far conceivable to differentiate and make a move in opposition to dirty automobiles.

8 IoT Security and Privacy

The most dangerous part of IoT is that consumers are giving up their privacy, bit by bit, without realizing it, because they do not know what data is collected and how it is used [109]. As a result, consumer privacy can be compromised and have no real remedied. Security and privacy illustration of IoT are given in Fig. 9 [110].

This helps to maintain the integrity of data and avoids hackers from examining it. All communication with your IoT devices must be authentic expending strong passwords or time-based authentication signs [111]. Antivirus

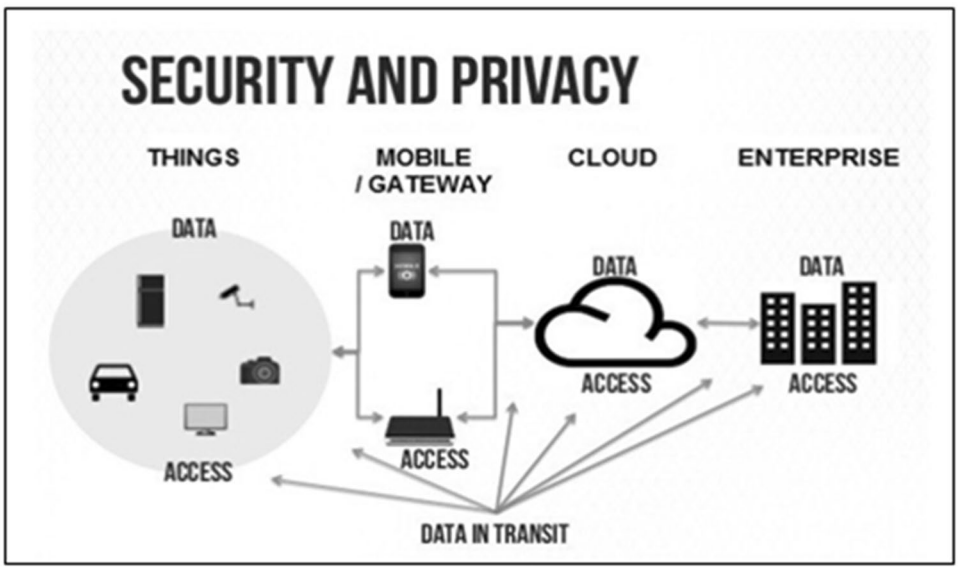

Fig. 9 Security and privacy of IoT

software can stipulate a critical layer of protection against outbreaks. Hardware, software, and connectivity must make sure secure for IoT objects that work more effectively [112]. Without the security in IoT or connect the objects from freezers to made artificial intelligence robots and also can be hacked by using ethical hacking [113]. Once hackers are gain control of your system, then you are not able to use your system until you connect them with some anti-virus tools. Make sure to protect your system from hackers that are more powerful than us, and they can assume the functionality of the object and steal the user's digital data.

Nowadays, anything can easily be hacked; so that we must secure our data and system otherwise we face many issues. Small systems are getting started with powerful IoT offerings. However, the security of their systems is to convince here, and devices connected to the Internet. It is important to get knowledge for how to protect your data is secure from hackers is a very important thing adopting advancements.

8.1 Risk 1: Storage of Personal Data

As with any technology, if there is security hole, hackers will try to promote openness. If a hacker can do it then you are not able to open your system Internet-connected devices that store credit card numbers or other personal information can be used as keys for small business networks. Many IoT devices exclusive data to generate various user-centric functions, and often leak it easily [114]. The nest, post office, and some codes were filtered out by the weather station near the thermostat.

8.2 Risk # 2: Lack of Regulations or Rules

As embedded attacks increase, developers must create a "problem-oriented approach (contacts are external)" to update IoT security and maintenance. Regular updates are needed, and identification and authentication management issues have made significant progress in reducing the risks associated with the IoT [115].

8.3 Risk # 3: Non-Existent Commitment to Updates and Security

When we choose IoT devices, we must make sure that it is a safe environment for our data and information. We must make sure for a safe environment and otherwise, our system can be hacked, and our private data is also can be a leak, so it is important to make our system safer for protecting our data otherwise it is a security risk [116].

8.4 Ways to Secure Your Data in IoT

8.4.1 # 1 Understand the Benefits of Connecting to the Internet

It is more important to make out the system first secure and then store our data in our system so, it is important to kind and be aware of this problem than so that the make of our system convinced that the make and model of the car and I will be there at home and then go to the gym and protect them from hackers.

8.4.2 # 2 Use the Secondary Network

Having a separate connection to act as a buffer will help ensure that no shared entity can access your shared files and other types of encrypted data. As with any technology, if there are security holes, hackers will try to promote openness, if a hacker can do it then you are not able to open your system keys for small business networks.

8.4.3 # 3 Keep Changing Your Passwords

We must change our password from time-to-time otherwise hackers can easily be able to get your password, and you face many problems in this way you must change your password from time to time.

8.4.4 # 4 Do not Enable Universal Plug and Play Functions

When we choose IoT devices, it is most important that we make sure that it is a safe environment otherwise, our system can be hacked easily, and our private data is also can be leak easily, so it is very important to make our system safer, and for protecting our data that is it is a big security risk.

8.5 Privacy Risk

- In IoT, devices are interconnected with different equipment and programming, so there are evident odds of touchy data spilling through unapproved control [117].
- All the devices are transmitting the client's very own data, for example, name, address, date of birth, wellbeing card data, charge card detail, and considerably more without encryption.
- Although there are security and protection worries with IoT, it adds esteems to our lives by permitting us to deal with our day by day schedule undertakings remotely

and naturally, and all the more critically, it is a distinct advantage for ventures [118].

8.5.1 Best IoT Security Practices

- Coming up next are other IoT security strategies you ought to consider executing [119].
- Plan decent border security with a firewall and an interruption counteraction framework.
- Remember everything for security data and occasion the board condition.
- Actualize a crisis reaction program.
- Incorporate a decent personality and access the executive's program with your IoT program for focal client control [120]. Consider, for example, utilizing a cloud personality approach.
- Actualize two-factor validation where handy.
- Have the executives of your devices utilize special client control.
- Quest for normalization. This is just in its early phases now, yet the market will before long characterize measures for the IoT, including security gauges.
- If you host a third-gathering IoT supplier, consider due ingenuity.
- Remain educated with key wellsprings of security through gatherings, for example, the National Institute of Standards and Technology (NIST).

8.6 IoT-Advantages

- *Better Customer Engagement* The current investigation is experiencing significant side effects and significant errors inaccuracy. Also, as referenced, commitment is inactive. IoT stabilizes it rapidly and gradually connects with the crowd.
- *Improving Technology* Similar developments and information that upgrade the client's experience also improve tool usage, and gradually add to powerful innovation. IoT opens a universe of important practical and field information [121].
- *Less Waste* IoT features territories of progress. Current examination outfits us with shallow bits of information; anyway, IoT gives veritable information that prompts progressively compelling resources to the board.
- *Improved Data Collection* Innovative for collecting data for passive use has its limitations and designs. IoT breaks it down from places and gives it a place where people want to go to analyze our world. It allows an accurate picture of everything [122].

8.7 IoT-Disadvantages

- *Security* Creates an ecosystem of constantly connected devices while interacting with IoT networks. Despite any security measures, this system provides little control. This exposes users to all sorts of attacks [123].
- *Complexity* A few people discover the IoT framework complex regarding plan, organization, and upkeep, given their utilization of a wide scope of innovations and an enormous assortment of new empowering advances [124].
- *Flexibility* Many people worry about the flexibility of the IoT system to easily integrate. They worry about finding themselves in several conflicting or closed systems.
- *Compliance* IoT, like any other technology in the realm of business, must comply with regulations. While many consider compliance with standard software to be a war, its complexity is incredibly challenging.
- *Marketing and Content Delivery* IoT improves this by watching more practices and breaking down them in an unexpected way. This prompts more data and detail, which gives increasingly solid measurements and examples.

It permits associations to more likely examine and react to client needs or inclinations.

9 Open Research Issues

The main purpose of this paper is to provide a review of IoT areas and research challenges. In this section, we discuss challenges and directions for future research work according to areas as we discussed earlier in this paper.

- *IoT Architecture* Still, there is no standardized architecture is provided by any researcher or organization [125]. The different researcher gives their ideas for architecture by using different types of sensors and technology according to their requirement, so there is need research work on IoT architecture to reach prominent architecture of IoT, which is acceptable for all applications. Multiple architectures of IoT may cause a problem in the future due to protocol issues in communication.
- *Technologies for IoT* In this research area still, a problem, what technology will be converted to IoT because it is feasible to convert agriculture, home, health, and supply chain management. There are few concerns about auto vehicles and health systems due to the failure to sensor it will cause a lot of damage [126]. System hardware for a particular field is also an issue because no prescribed hardware or software is recognized by researchers or organizations. Communication route is also a problem

because most IoT applications were used from smartphones, and during mobility, the cell is changed, and the route of communication is also changed this will cause a delay to send an instruction to the IoT system for particular action this is a big issue [127].

- *Cloud IoT* IoT devices generate big data, which will be sent to the cloud for the process this will cause delays for results and action due to communication delay from the cloud to the IoT device [128]. The distance of the cloud from IoT devices is also causing delays in sending and receiving data. It is also a big problem that a simple IoT system required storage of log files and data of transactions or related to applications, so cloud storage purchasing also increases the cost of cloud IoT systems.
- *Fog IoT* IoT sensors continuously generate sensitive data of monitoring to send cloud for analysis and acting on contorted situations, but the cloud is far away from the IoT system. Transfer of huge amounts of data from IoT devices to the cloud takes time for transfer and analysis, so this is not good for real-time applications. Fog computing provides processing at the edge of IoT sensors but, the transfer of data is a problem due to lack of security, trusted and untrusted nodes [129, 130]. The fog did not provide hefty data storage like the cloud and cannot save for a long time, so this is also a big problem of Fog IoT [131].
- *IoT applications* IoT applications were developed by many researchers and organizations but, the quality of experience (QoE) of users was not considered yet to improve their quality of service (QoS) [132, 133]. Merging QoE in IoT applications will help the developer to develop applications according to user's needs and as well as service providers to help improve service preferences according to user needs [134].

10 Conclusion

In this paper, we studied IoT and supporting technologies such as cloud, fog, 6G, and applications. Further, we provide architecture, security, and privacy of IoT. Security and privacy of IoT applications are important for data securing and avoid loss. Advantages and disadvantages and open research issues are also discussed for future research directions. We found that sensors are important components of the IoT system; if sensors fail during the monitoring of the environment or controlling a vehicle or in health applications, it will cause serious damage. We provide definitions of the key concept and background, and types of IoT applications, utilization for future development has also been presented.

Acknowledgements This research was supported in part by the China NSFC Grant (U2001207, 61872248), Guangdong NSF 2017A030312008, Shenzhen Science and Technology Foundation (No. ZDSYS20190902092853047), the Project of DEGP (No.2019KCXTD005), the Guangdong "Pearl River Talent Recruitment Program" under Grant 2019ZT08X603. Kaishun Wu is the corresponding author.

Declarations

Conflict of interest Authors did not have any conflict of interest.

References

1. Thumeera WR, Gosine RG, James LA, Mann GKI, de Silva O, Warrian PJ (2020) The internet of things in the oil and gas industry: a systematic review. IEEE Internet Things J
2. Aloi G, Caliciuri G, Fortino G, Gravina R, Pace P, Russo W, Savaglio C (2017) Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. J Netw Comput Appl 81:74–84
3. Zhou W, Jia Y, Peng A, Zhang Y, Liu P (2018) The effect of iot new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J 6(2):1606–1616
4. David R (2014) Enchanted objects: design, human desire, and the internet of things. Simon and Schuster
5. Warwick BR, Haslett AM (2018) Method and system of monitoring appliance usage. U.S. Patent Application 15/552,087. Filed 1 Feb 2018
6. Krishna V (2020) IoT sensor market. https://communalnews.com/ms/pasaran-sensor-iot/. Accessed 20 Nov 2020
7. Sahni Y, Cao J, Zhang S, Yang L (2017) Edge mesh: a new paradigm to enable distributed intelligence in internet of things. IEEE Access 5:16441–16458
8. Medhat GM, Aneiba A, Basurra S, Batty O, Elmisery AM, Kovalchuk Y, Rehman MHU (2019) Internet of things and data mining: from applications to techniques and systems. Wiley Interdiscip Rev Data Min Knowl Disc 9(3):e1292
9. Wei Z, Jia Y, Yao Y, Zhu L, Guan L, Mao Y, Liu P, Zhang Y (2019) Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms. In: 28th {USENIX} security symposium ({USENIX} security 19, pp 1133–1150
10. Fatima H, Hussain R, Hassan SA, Hossain E (2020) Machine learning in IoT security: current solutions and future challenges. IEEE Commun Surv Tut
11. Francesco P, Cuomo S, di Cola VS, Casolla G (2019) A machine learning approach for IoT cultural data. J Amb Intel Hum Comput 1–12
12. Hossein MN, Taleb T, Arouk O (2016) Low-altitude unmanned aerial vehicles-based internet of things services: comprehensive survey and future perspectives. IEEE Internet Things J 3(6):899–922
13. Marjani M, Nasaruddin F, Gani A, Karim A, Hashem IAT, Siddiqa A, Yaqoob I (2017) Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access 5:5247–5261
14. Akbar A, Kousiouris G, Pervaiz H, Sancho J, Ta-Shma P, Carrez F, Moessner K (2018) Real-time probabilistic data fusion for large-scale IoT applications. IEEE Access 6:10015–10027
15. https://www.gadgetaffairs.com/author/admin/. Accessed 18 Nov 2020
16. Sarah AA, Almulhim HA, Almulhim MF, Chaudhry SR (2016) IoT architecture challenges and issues: lack of standardization.

In: 2016 future technologies conference (FTC). IEEE, pp 731–738
17. Arpan P, Rath HK, Shailendra S, Bhattacharyya A (2018) IoT standardization: the road ahead. In: Internet of things-technology, applications and standardization. IntechOpen, pp 53–74
18. Bader SR, Maleshkova M, Lohmann S (2019) Structuring reference architectures for the industrial internet of things. Futur Internet 11(7):151
19. de Cleber MM, Sadok D, Kelner J (2019) An IoT sensor and scenario survey for data researchers. J Br Comput Soc 25(1):4
20. Albrecht S, Van Laerhoven K (2001) How to build smart appliances? IEEE Pers Commun 8(4):66–71
21. Khelifi F, Bradai A, Benslimane A, Rawat P, Atri M (2019) A survey of localization systems in internet of things. Mob Netw Appl 24(3):761–785
22. Andrews LJ, Baptist LR, Shanmugasundaram S (2019) Mobile android-based remote patient monitoring system through wearable sensors. J Discr Math Sci Cryptogr 22(4):557–568
23. Damien D (2019) Examining neural reactivity to gambling cues in the age of sports betting. J Behav Addict
24. Benitez-Andonegui A, Burden R, Benning R, Möckel R, Lührs M, Sorger B (2020) An augmented-reality fNIRS-based brain-computer interface: a proof-of-concept study. Front Neurosci 14:346
25. Vijaya SR, Nalluri S, Ramasubbareddy S, Govinda K, Swetha E (2020) Brilliant corp yield prediction utilizing internet of things. Data engineering and communication technology. Singapore: Springer, pp 893–902
26. Salah MK (2019) IoT physical layer: sensors, actuators, controllers and programming. The Era of Internet of Things. Cham: Springer, pp 21–47
27. Wen C, Wu H, Dayong TANG, Zhang E, Cao L, Shi R (2019) Method and apparatus for reducing continuous-wakeup delay of bluetooth loudspeaker, and bluetooth loudspeaker. U.S. Patent Application 16/369,456. Filed 3 Oct 2019
28. Jonathan T, Lesueur F, Le Mouël F, Guyon L, Ben-Hassine H (2020) A survey of IoT protocols and their security issues through the lens of a generic IoT stack. Internet of Things 100264
29. Jin-Shyan L, Dong M-F, Sun Y-H (2015) A preliminary study of low power wireless technologies: ZigBee and bluetooth low energy. In: 2015 IEEE 10th conference on industrial electronics and applications (ICIEA). IEEE, pp 135–139
30. Giancarlo F, Savaglio C, Palau CE, de Puga JS, Ganzha M, Paprzycki M, Montesinos M, Liotta A, Llop M (2018) Towards multi-layer interoperability of heterogeneous IoT platforms: the INTER-IoT approach. Integration, interconnection, and interoperability of IoT systems. Cham: Springer, pp 199–232
31. https://camrojud.com/how-iot-works-4-main-components-of-iot-system/. Accessed 6 Jun 2020
32. Gwani SM, Sequeiros JBF, Correia AFPP, Freire M, Inacio PRM (2017) IoT hardware development platforms: past, present, and future. Internet Things-Chall Adv Appl 101–133
33. Petrov V, Samuylov A, Begishev V, Moltchanov D, Andreev S, Samouylov K, Koucheryavy Y (2017) Vehicle-based relay assistance for opportunistic crowdsensing over narrowband IoT (NB-IoT). IEEE Internet Things J 5(5):3710–3723
34. Julia J (2017) Internet of things based Deadbolt lock latch strike location smart sensor. U.S. Patent Application 14/804,146. Filed 26 Jan 2017
35. Adegbija T, Rogacs A, Patel C, Gordon-Ross A (2017) Microprocessor optimizations for the internet of things: a survey. IEEE Trans Comput Aid Des Integr Circ Syst 37(1):7–20
36. Tsai C-W, Lai C-F, Vasilakos AV (2014) Future internet of things: open issues and challenges. Wireless Netw 20(8):2201–2217
37. Efremov S, Pilipenko N, Voskov L (2015) An integrated approach to common problems in the internet of things. Procedia Eng 100:1215–1223
38. Fatmasari RL, Ozcelebi T, Lukkien J (2018) Understanding IoT systems: a life cycle approach. Procedia Comput Sci 130:1057–1062S
39. Qian Z, Wang R, Chen Q, Liu Y, Qin W (2010) Iot gateway: bridging wireless sensor networks into internet of things. In: 2010 IEEE/IFIP international conference on embedded and ubiquitous computing. IEEE, pp 347–352
40. Hamrioui S, Lorenz P (2017) Bio inspired routing algorithm and efficient communications within IoT. IEEE Netw 31(5):74–79
41. Sachin B, Stango A, Prasad N, Sen J, Prasad R (2011) Proposed embedded security framework for internet of things (iot). In: 2011 2nd international conference on wireless communication, vehicular technology, information theory and aerospace and electronic systems technology (wireless VITAE). IEEE, pp 1–5
42. Das Almeida RJ, Brito V, Palma LB, Barata J (2017) Approach to adapt a legacy manufacturing system into the IoT paradigm. Int J Interact Mob Technol iJIM 11(5)
43. Jasmin G, Breitenbücher U, Falkenthal M, Leymann F, Reinfurt L (2016) Comparison of IoT platform architectures: a field study based on a reference architecture. In: 2016 cloudification of the internet of things (CIoT). IEEE, pp 1–6
44. Rodger L, Blackstock M (2014) City hub: a cloud-based IoT platform for smart cities. In: 2014 IEEE 6th international conference on cloud computing technology and science, pp 799–804. IEEE, 2014.
45. Mohieddine B, Abdaoui A, Ahmad SHM, Touati F, Kadri A (2018) A modular IoT platform for real-time indoor air quality monitoring. Sensors 18(2):581
46. Hamdan H, Rajab H, Cinkler T, Lengyel L (2018) Survey of platforms for massive IoT. In: 2018 IEEE international conference on future IoT technologies (future IoT). IEEE, pp 1–8
47. Sruthy S, George SN (2017) WiFi enabled home security surveillance system using Raspberry Pi and IoT module. In: 2017 IEEE international conference on signal processing, informatics, communication and energy systems (SPICES), IEEE, pp 1–6
48. Centenaro M, Vangelista L, Zanella A, Zorzi M (2016) Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. IEEE Wirel Commun 23(5):60–67
49. Rashid N, Ahmed Z, Ahmad Z, Shaikh N, Laghari A, Kumar K (2020) Cloud computing applications: a review. EAI Endor Trans Cloud Syst 6(17)
50. Mahalle PN, Shinde GR, Deshpande AV (2021) The convergence of internet of things and cloud for smart computing. CRC Press
51. Ali LA, He H, Khan A, Kumar N, Kharel R (2018) Quality of experience framework for cloud computing (QoC). IEEE Access 6:64876–64890
52. Stergiou C, Psannis KE, Kim B-G, Gupta B (2018) Secure integration of IoT and cloud computing. Futur Gener Comput Syst 78:964–975
53. Pacheco PG, Prazeres C (2019) Web of things data visualization: from devices to web via fog and cloud computing. In: 2019 IEEE 28th international conference on enabling technologies: infrastructure for collaborative enterprises (WETICE). IEEE, pp 140–145
54. Gregory BE, Chao J (2020) Recovery strategy for a stream processing system. U.S. Patent Application 16/793, 936. Filed 11 Jun 2020
55. Hosuk L-M (2018) Stealing thunder: cloud, IoT and 5G will change the strategic paradigm for protecting European commercial interests. Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness? No. 2/18. ECIPE Occasional Paper.

56. Gunaseelan JSK, Ellappan V (2017) IOT agriculture to improve food and farming technology. In: 2017 conference on emerging devices and smart systems (ICEDSS). IEEE, pp 260–266
57. Ammar R, Salam S (2017) Internet of things from hype to reality. The road to digitization; River Publisher Series in Communications, Springer: Basel, Switzerland 49
58. Philip W (2018) Practical guide to salesforce communities: building, enhancing, and managing an online community with salesforce community cloud. Apress
59. https://venturebeat.com/2015/09/15/salesforce-launches-iot-cloud-to-let-business-users-act-on-big-data/. Accessed 24 Nov 2020
60. Jeet KM, Riaz S, Mushtaq A (2020) Cyber-physical cloud computing systems and internet of everything. In: Principles of internet of things (IoT) ecosystem: insight paradigm. Cham: Springer, pp 201–227
61. Mamdouh A, Almustafa K, Meerja KA (2019) Cloud based SDN and NFV architectures for IoT infrastructure. Egyptian Inform J 20(1):1–10
62. Krishna SS, Wang X (2017) Live data analytics with collaborative edge and cloud processing in wireless IoT networks. IEEE Access 5:4621–4635
63. Ali LA, He H, Memon KA, Laghari RA, Halepoto IA, Khan A (2019) Quality of experience (QoE) in cloud gaming models: a review. Multiagent Grid Syste 5(3):289–304
64. Farshad F, Farahani B (2020) Architecting IoT Cloud. Intel internet things. Cham: Springer, pp 173–241
65. Ali LA, He H, Shafiq M, Khan A (2016) Assessing effect of cloud distance on end user's quality of experience (QoE). In: 2016 2nd IEEE international conference on computer and communications (ICCC). IEEE, pp 500–505
66. Vishal K, Laghari AA, Karim S, Shakir M, Brohi AA (2019) Comparison of fog computing and cloud computing. Int J Math Sci Comput (IJMSC) 5(1):31–41
67. Adeel A, Deng Z, Memon KA, Laghari AA, Mohammadani KH (2019) A dynamic application-partitioning algorithm with improved offloading mechanism for fog cloud networks. Futur Internet 11(7):141
68. Puliafito C, Mingozzi E, Longo F, Puliafito A, Rana O (2019) Fog computing for the internet of things: a survey. ACM Trans Internet Technol (TOIT) 19(2):1–41
69. Hina M, Lei LH, Laghari AA, Karim S (2020) Quality of Experience and quality of service of gaming services in fog computing. In: Proceedings of the 2020 4th international conference on management engineering, software engineering and service sciences. pp 225–228
70. Mohit T, Davy A (2017) Resource aware placement of IoT application modules in fog-cloud computing paradigm. In: 2017 IFIP/IEEE symposium on integrated network and service management (IM). IEEE, pp 1222–1228
71. Ali LA, Jumani AK, Laghari RA (2021) Review and state of art of fog computing. Arch Comput Method Eng 1–13
72. Tuz ZF, Khan MRR, Bhuiyan MFR, Das AK (2017) Enhancing the capabilities of IoT based fog and cloud infrastructures for time sensitive events. In: 2017 International conference on electrical engineering and computer science (ICECOS). IEEE, pp 224–230
73. Amir MR, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, Liljeberg P (2018) Exploiting smart e-Health gateways at the edge of healthcare internet-of-things: a fog computing approach. Futur Gener Comput Syst 78:641–658
74. Viejo A, Sánchez D (2020) Secure monitoring in IoT-based services via fog orchestration. Futur Gener Comput Syst 107:443–457
75. Ahmad K, Siddiqa A, Safdar Z, Razzaq M, Gillani SA, Tahir H, Kiran S, Ahmed E, Imran M (2020) Big data management in participatory sensing: issues, trends and future directions. Futur Gener Comput Syst 107:942–955
76. Xuebing D, Chang Y, Wang Y, Yan J (2017) Understanding usage of internet of things (IOT) systems in China. Inf Technol People
77. Faisal T, Khandaker MRA, Wong K-K, Imran MA, Bennis M, Debbah M (2020) A speculative study on 6G. IEEE Wirel Commun 27(4):118–125
78. Qiao Q, Chen X, Zhong C, Zhang Z (2020) Integration of energy, computation and communication in 6G cellular internet of things. IEEE Commun Lett
79. Saad W, Bennis M, Chen M (2019) A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Netw 34(3):134–142
80. Calvanese SE, Barbarossa S, Gonzalez-Jimenez JL, Ktenas D, Cassiau N, Maret L, Dehos C (2019) 6G: the next frontier: from holographic messaging to artificial intelligence using subterahertz and visible light communication. IEEE Vehic Technol Magaz 14(3):42–50
81. Zaman CM, Shahjalal M, Ahmed S, Jang YM (2020) 6G wireless communication systems: applications, requirements, technologies, challenges, and research directions. IEEE Open J Commun Soc 1:957–975
82. Zhang Z, Xiao Y, Ma Z, Xiao M, Ding Z, Lei X, Karagiannidis GK, Fan P (2019) 6G wireless networks: vision, requirements, architecture, and key technologies. IEEE Veh Technol Mag 14(3):28–41
83. Deebak BD, Fadi A-T (2020) Drone of IoT in 6G wireless communications: technology, challenges, and future aspects. Unmanned aerial vehicles in smart cities. Cham: Springer, pp 153–165
84. Ciro F, Pavia D, Gurgen L, Yonezawa T, Galache JA, Doguchi K, Matranga I (2015) The advantages of IoT and cloud applied to smart cities. In: 2015 3rd international conference on future internet of things and cloud. IEEE, pp 325–332
85. Aditya T, Mahato M, Chidar A, Chandrol MK, Shrivastava M, Tripathi M (2018) Internet of things (IoT): research, architectures and applications. Int J Futur Revol Comput Sci Commun Eng 4(3):23–27
86. Ud DK, Guizani M, Hassan S, Kim B-S, Khan MK, Atiquzzaman M, Ahmed SH (2018) The internet of things: a review of enabled technologies and future challenges. IEEE Access 7:7606–7640
87. Samir C, Byun J, Dutta K, Pedersen RU, Pottathil A, Xie H (2018) Designing an internet-of-things (IoT) and sensor-based in-home monitoring system for assisting diabetes patients: iterative learning from two case studies. Eur J Inf Syst 27(6):670–685
88. Benjamin KS, Furszyfer Del Rio DD (2020) Smart home technologies in Europe: a critical review of concepts, benefits, risks and policies. Renew Sustain Energy Rev 120:109663
89. Jana S, Waheed A (2019) Role of smart wearable in healthcare: wearable internet of medical things (WIoMT). The IoT and the next revolutions automating the world. IGI Global, pp 133–155
90. Nina C, Trilar J, Kos A, Volk M, Duh ES (2020) The use of IoT technology in smart cities and smart villages: similarities, differences, and future prospects. Sensors 20(14):3897
91. González GC, Meana-Llorián D, Pelayo G-Bustelo BC, Lovelle JMC, Garcia-Fernandez N (2017) Midgar: detection of people through computer vision in the internet of things scenarios to improve the security in smart cities, smart towns, and smart homes. Futur Gener Comput Syst 76:301–313
92. Hasna U, Gibson M, Safdar MA, Kalsoom T, Ramzan N, Ur-Rehman M, Imran MA (2019) IoT for 5G/B5G applications in smart homes, smart cities, wearables and connected cars. In: 2019 IEEE 24th international workshop on computer aided modeling and design of communication links and networks (CAMAD). IEEE, , pp 1–5

93. László L, Ekler P, Ujj T, Balogh T, Charaf H (2015) SensorHUB: an IoT driver framework for supporting sensor networks and data analysis. Int J Distrib Sens Netw 11(7):454379
94. Fernández-Caramés TM, Fraga-Lamas P (2018) Towards the Internet of smart clothing: a review on IoT wearables and garments for creating intelligent connected e-textiles. Electronics 7(12):405
95. Indrakumari R, Poongodi T, Suresh P, Balamurugan B (2020) The growing role of internet of things in healthcare wearables. In: Emergence of pharmaceutical industry growth with industrial IoT approach. Academic Press, pp 163–194
96. Athul J (2017) Smart retail 4.0 IoT consumer retailer model for retail intelligence and strategic marketing of in-store products. In: Proceedings of the 17th international business horizon-INBUSH ERA-2017, Noida, India 9
97. Shu-Hsien L, Yang L-L (2020) Mobile payment and online to offline retail business models. J Retail Consum Serv 57:102230
98. Amine R, Oumnad A (2018) Challenges and opportunities of internet of things in healthcare. Int J Electr Comput Eng 8:2088–8708
99. Ricardo SA, Sittón-Candanedo I, García O, Prieto J, Rodríguez-González S (2020) An intelligent Edge-IoT platform for monitoring livestock and crops in a dairy farming scenario. Ad Hoc Netw 98:102047
100. Shoaib FM, Riaz S, Abid A, Abid K, Naeem MA (2019) A survey on the role of IoT in agriculture for the implementation of smart farming. IEEE Access 7:156237–156271
101. Ben-Daya M, Hassini E, Bahroun Z (2019) Internet of things and supply chain management: a literature review. Int J Prod Res 57(15–16):4719–4742
102. Leminen S, Rajahonka M, Wendelin R, Westerlund M (2020) Industrial internet of things business models in the machine-to-machine context. Ind Mark Manag 84:298–311
103. Zaidan AA, Zaidan BB (2020) A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. Artif Intel Rev 53(1):141–165
104. Pravin K, More V, Hendre V, Chippalkatti P, Paliwal K (2020) IOT based baby incubator for clinic. In ICCCE 2019. Singapore: Springer, pp 349–355
105. Pushpanjali K, Goel P, Reddy SRN (2015) PiCam: IoT based wireless alert system for deaf and hard of hearing. In: 2015 international conference on advanced computing and communications (ADCOM). IEEE, pp 39–44
106. Guenter H-D, Idris E (2006) Smart water metering. Water 33(3):38–41
107. Sanjeevi P, Prasanna S, Siva Kumar B, Gunasekaran G, Alagiri I, Vijay Anand R (2020) Precision agriculture and farming using internet of things based on wireless sensor network. Trans Emerg Telecommun Technol e3978
108. Manna S, Bhunia SS, Mukherjee N (2014) Vehicular pollution monitoring using loT. IEEE, pp 2214–2220
109. Bryan FC, Foltz L (2020) Mobile users' information privacy concerns instrument and IoT. Inf Comput Secur
110. Prabhjot S (2018) Cross-layer design for internet of things (IOT)-issues and possible solutions. Dep Syst Comput Eng 1–10
111. Vidya R, Prema KV (2019) Light-weight hashing method for user authentication in internet-of-things. Ad Hoc Netw 89:97–106
112. Mfanasibili N, Ngoepe M (2020) A framework for data security, privacy, and trust in "consumer internet of things" assemblages in South Africa. Secur Priv e122
113. Christopher R, Toft J (2019) Finding vulnerabilities in IoT devices: ethical hacking of electronic locks
114. David JW, Taly A, Shankar A, Boneh D (2016) Privacy, discovery, and authentication for the internet of things. In: European symposium on research in computer security. Cham: Springer, pp 301–319
115. Ricardo N, Steri G, Baldini G (2014) Enforcement of security policy rules for the internet of things. In: 2014 IEEE 10th international conference on wireless and mobile computing, networking and communications (WiMob). IEEE, pp 165–172
116. Jibran S, Hammoudeh M, Raza U, Adebisi B, Ande R (2018) IoT standardisation: challenges, perspectives and solution. In: Proceedings of the 2nd international conference on future networks and distributed systems, pp 1–9
117. Ajiji YM (2020) Internet of thing (IOT): data and information (gadget protection). J Appl Sci Eng Technol Educ 2(2):194–203
118. Shivani P, Shah M (2020) A comprehensive study on critical security issues and challenges of the IoT world. J Data Inf Manag 1–22
119. Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N (2019) Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Commun Surv Tut 21(3):2702–2733
120. Hamid MA, Khaleefah RM, Abdulateef IA (2020) a review software defined networking for internet of things. In: 2020 international congress on human-computer interaction, optimization and robotic applications (HORA). IEEE, pp 1–8
121. Daniel M, Occhiogrosso B (2019) Practical aspects for the integration of 5G networks and IoT applications in smart cities environments. Wirel Commun Mob Comput 2019
122. Gregory G (2020) Bringing dark data into the light: illuminating existing IoT data lost within your organization. Bus Horiz
123. Hassan WH (2019) Current research on internet of things (IoT) security: a survey. Comput Netw 148:283–294
124. Francesco C, Cinelli L, Corradini E, Terracina G, Ursino D, Virgili L, Fortino G, Liotta A, Savaglio C (2020) A framework for anomaly detection and classification in Multiple IoT scenarios. Futur Gener Comput Syst
125. Baha R, Alam T, Eskicioglu R (2020) The next generation internet of things architecture towards distributed intelligence: reviews, applications, and research challenges. J Telecommun Electr Comput Eng (JTEC) 12(2)
126. Guilin Z, Xing L (2020) Reliability analysis of IoT systems with competitions from cascading probabilistic function dependence. Reliab Eng Syst Saf 106812
127. An C, Celimuge W (2020) Traffic big data assisted V2X communications toward smart transportation. Wirel Netw 26(3):1601–1610
128. Paolo F, Flammini A, Sisinni E, Rinaldi S, Brandão D, Rocha MS (2018) Delay estimation of industrial IoT applications based on messaging protocols. IEEE Trans Instr Measur 67(9):2188–2199
129. Zhang P, Zhou M, Fortino G (2018) Security and trust issues in Fog computing: a survey. Futur Gener Comput Syst 88:16–27
130. Gu K, Na W, Yin B, Jia W (2019) Secure data query framework for cloud and fog computing. IEEE Trans Netw Serv Manag 17(1):332–345
131. Shikhar V, Kawamoto Y, Fadlullah ZM, Nishiyama H, Kato N (2017)A survey on network methodologies for real-time analytics of massive IoT data and open research issues. IEEE Commun Surv Tut 19(3):1457–1477
132. Ali LA, He H, Shafiq M, Khan A (2019) Application of quality of experience in networked services: review, trend and perspectives. Syst Pract Act Res 32(5):501–519
133. Redowan M, Srirama SN, Ramamohanarao K, Buyya R (2019) Quality of experience (QoE)-aware placement of applications in Fog computing environments. J Parallel Distrib Comput 132:190–203
134. Ali LA, Memon KA, Soomro MB, Laghari RA, Kumar V (2020) Quality of experience (QoE) assessment of games on workstations and mobile. Entertain Comput 100362