sustainability

Review

Revolutionary Strategies Analysis and Proposed System for Future Infrastructure in Internet of Things

Arun Kumar [1], Sharad Sharma [1], Aman Singh [2], Ayed Alwadain [3], Bong-Jun Choi [4,5,*], Jose Manual-Brenosa [6,7], Arturo Ortega-Mansilla [6,7] and Nitin Goyal [8,*]

[1] Department of Electronics and Communication Engineering, Maharishi Markandeshwar (Deemed to be University), Mullana 133203, India; ranaarun1.ece@piet.co.in (A.K.); sharadpr123@rediffmail.com (S.S.)
[2] School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India; amansingh.x@gmail.com
[3] Computer Science Department, Community College, King Saud University, Riyadh P.O. Box 145111, Saudi Arabia; aalwadain@ksu.edu.sa
[4] School of Computer Science & Engineering, Soongsil University, Seoul 06978, Korea
[5] School of Electronic Engineering, Soongsil University, Seoul 06978, Korea
[6] Higher Polytechnic School, Universidad Europea del Atlántico, C/Isabel Torres 21, 39011 Santander, Spain; josemanuel.brenosa@uneatlantico.es (J.M.-B.); arturo.ortega@uneatlantico.es (A.O.-M.)
[7] Department of Project Management, Universidad Internacional Iberoamericana, Campeche 24560, Mexico
[8] Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura 140401, India
[*] Correspondence: davidchoi@soongsil.ac.kr (B.-J.C.); dr.nitingoyal30@gmail.com (N.G.)

Abstract: The Internet of Things (IoT) has changed the worldwide network of people, smart devices, intelligent things, data, and information as an emergent technology. IoT development is still in its early stages, and numerous interrelated challenges must be addressed. IoT is the unifying idea of embedding everything. The Internet of Things offers a huge opportunity to improve the world's accessibility, integrity, availability, scalability, confidentiality, and interoperability. However, securing the Internet of Things is a difficult issue. The IoT aims to connect almost everything within the framework of a common infrastructure. This helps in controlling devices and, will allow device status to be updated everywhere and at any time. To develop technology via IoT, several critical scientific studies and inquiries have been carried out. However, many obstacles and problems remain to be tackled in order to reach IoT's maximum potential. These problems and concerns must be taken into consideration in different areas of the IoT, such as implementation in remote areas, threats to the system, development support, social and environmental impacts, etc. This paper reviews the current state of the art in different IoT architectures, with a focus on current technologies, applications, challenges, IoT protocols, and opportunities. As a result, a detailed taxonomy of IoT is presented here which includes interoperability, scalability, security and energy efficiency, among other things. Moreover, the significance of blockchains and big data as well as their analysis in relation to IoT, is discussed. This article aims to help readers and researchers understand the IoT and its applicability to the real world.

Keywords: architecture; communication protocol; enabling technologies; interoperability

check for updates

Citation: Kumar, A.; Sharma, S.; Singh, A.; Alwadain, A.; Choi, B.-J.; Manual-Brenosa, J.; Ortega-Mansilla, A.; Goyal, N. Revolutionary Strategies Analysis and Proposed System for Future Infrastructure in Internet of Things. *Sustainability* **2022**, *14*, 71. https://doi.org/10.3390/su14010071

Academic Editor: Simon Elias Bibri

Received: 16 October 2021
Accepted: 13 December 2021
Published: 22 December 2021

1. Introduction

The Internet of Things (IoT) is a concept that connects physical items to the Internet, allowing them to gather, process, and transfer data without the need for human interaction. The objective of the Internet of Things is to build a better environment for people in which items (physical objects; terminology such as an object, gadget, entity, and thing are interchangeable) around us can understand our preferences and likeness and act properly without explicit instructions. The exponential rise of the Internet of Things has been aided by significant advancements in low-cost sensor manufacture, communication protocols, embedded systems, actuators, and hardware downsizing. The cumulative user base of linked IoT devices is expected to hit one trillion devices worldwide by 2025, a five-fold increase in ten years, as shown in Figure 1. IoT is a vast collection of smart embedded devices that are connected to the Internet and provide unique services to meet the needs of users [1]. IoT represents a transition from simply connecting end-user devices to the Internet to using the Internet to connect smart objects (also known as IoT devices) and allow them to communicate with one another and/or with humans while including a diverse set of applications and services. IoT platforms typically deploy a large number of smart devices, such as wearable sensors, Radio frequency identification system (RFID) devices and actuators to remotely control various physical, environmental and physiological quantities [2]. IoT, which is based on the computer Internet, actually establishes the Internet by relying on RFID and radio data transfer technology to connect things. As a result, RFID is one of the most important IoT fundamental technologies. Things are allowed to communicate with each other within this network without the need for human intervention. The foundation of the Internet of Things is the automatic identification of objects as well as their interconnection and sharing of information via the computer Internet, which is based on RFID technology, which itself is simply a technology that allows objects to "talk." RFID tags are used in the IoT phase to store information with laws and interoperability that is automatically recorded in a central information system via a radio data communication system, allowing things to be identified and information to be exchanged and shared via the open Internet. To empower diverse remote monitoring systems, IoT devices often run in a long-term mode and connect wirelessly with each other and with a central fusion node. Remote sensing systems are typically battery-powered; limited battery power affects the system's efficiency, which leads to lower integration and consumer compliance [3]. To address these constraints, acquired data should first be compressed before being sent to a fusion center using optimized paths to reduce high energy utilization. Advanced data compression and transmission techniques normally consume a significant amount of onboard energy; therefore, the chosen compression method must be able to provide long-term reliable monitoring while still reducing power consumption [4]. Intelligent applications have been stretched from humans to the things that surround humans as information technology has progressed. Sensor networks, the Internet, mobile communications, cloud computing, intelligent information processing, and other established networking and information technologies are all part of the Internet of Things. By establishing an isomerous link between core and terminal networks, the Internet of Things focuses on information service, combining computer systems with observation of the physical world, cognition, influence, and control. The real, digital and virtual worlds, as well as human perception, are all connected.

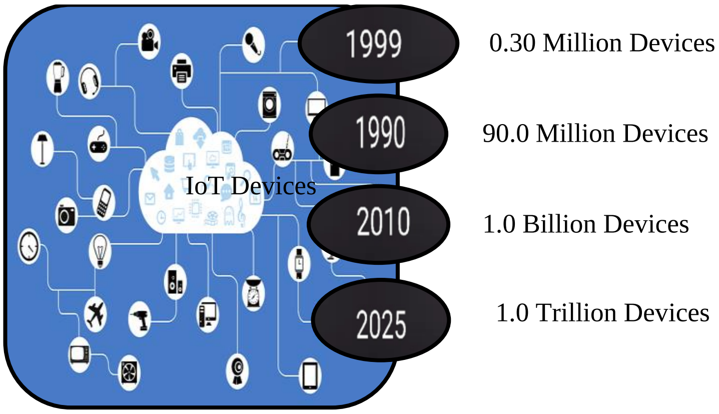


Figure 1. Number of IoT devices till 2025.

As a result, there is no common concept of the Internet of Things, and current visions are unclear. The Internet of Things (IoT) is focused on the convergence of various standards and enabling technologies with various sensing, networking, storage, computing, and other capabilities [5]. However, because of the fragmentation of standards and the diversity of deployed technologies, ensuring the complete connectivity of all is a major challenge. As a result, one of the major challenges of IoT growth is dynamic integration. Many standardization organizations, partnerships, academics and industries are working on IoT growth, innovation and standardization; however, there is still a need for a holistic system with integrated standards under a single IoT vision [6].

The IoT has much to offer in different fields of life and technology. IoT has a great deal of potential in terms of both enhancing technology and facilitating human beings. Therefore, the IoT is a contemporary model that connects the next generation of technological advances with a collection of existing facilities. IoT technologies are almost infinite, thus allowing the cyber-world to easily merge with the real world [7]. However, despite the tremendous efforts of standardization agencies, associations, sectors, academics, and others, various challenges still need to be solved in order to achieve the full capacity of the IoT. Such problems should be viewed from multiple angles, such as technology support, implementation, and market models as well as social and environmental effects. Many of the major problems facing IoT contribute to traffic loads and different traffic models [8]. More and more devices are connecting to the Internet each day, and devices are becoming the main producers and consumers of traffic. This gives rise to traffic specifications and the need for new traffic models, protocols, network capacities, protection measures, etc. Simplification is required, and adoption of new Internet Protocol (IP) architecture enables smooth networking and efficient management in the heterogeneous network (HetNet) environment [9].

Some other IoT technology issues include system recognition, addressing, interoperability, usability, management, energy consumption, stability, privacy, large scales and more. In addition, potential IoT implementations need to achieve a sustainable smart planet with an emphasis on green IoT supporting technology, which is another major issue. With recent developments in internet technologies, IoT technology is gradually affecting our everyday lives and starting to deliver fascinating and beneficial new services. According to the key IoT visions and supporting technologies, this article includes reports on the state of the art, emerging developments, and open issues [10]. Blockchains, or decentralized distributed ledgers, are a game-changing technology that might help solve IoT security issues. A blockchain-based approach to IoT networks might address many of the issues with the existing paradigm while also increasing security [11]. The use of blockchains in IoT security allows for direct information exchange between connected devices rather than communicating through a centralized network, reducing the IoT's vulnerability to cyber-attacks. According to a Gartner report, healthcare, transportation, and energy have the greatest rates of blockchain use among IoT-enabled firms in the United States. As a result, this paper provides readers with helpful guidelines for understanding the IoT paradigm and related open problems, as well as potential research and development opportunities [12].

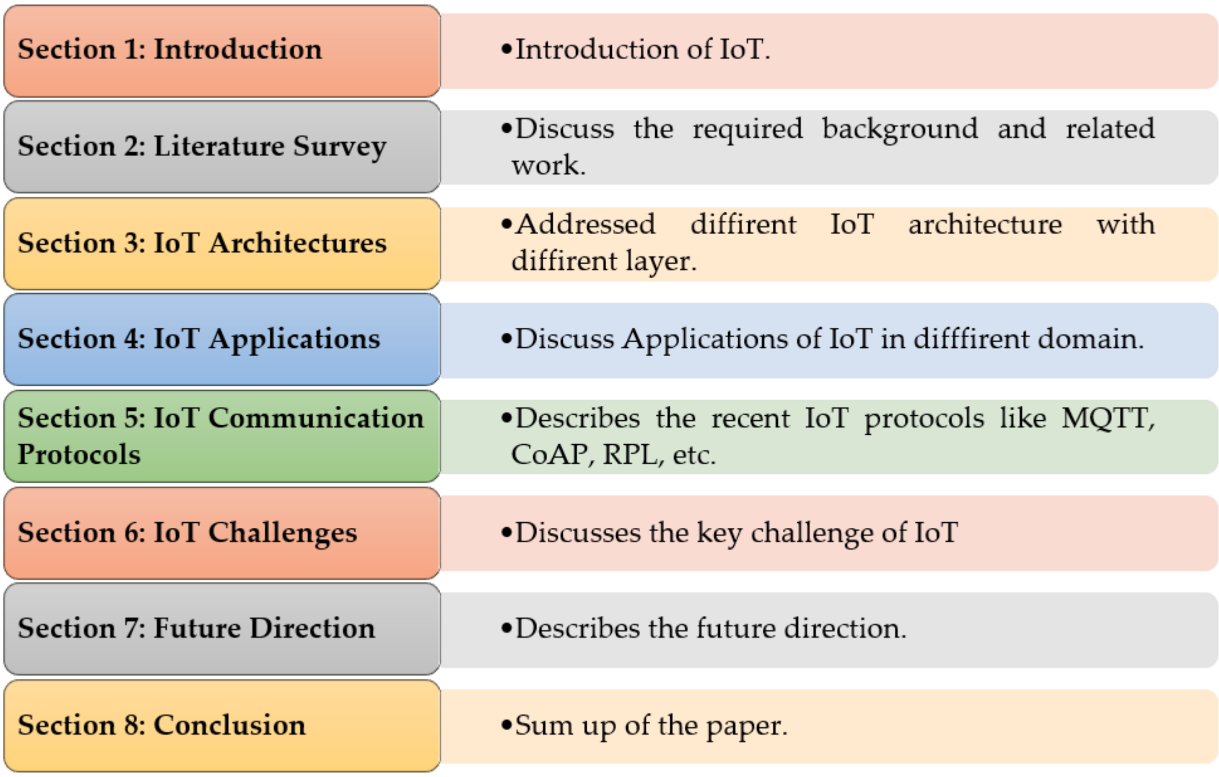
The principal contribution of this article is to determine the scope, depth and variety of current IoT research. The rapid development of IoT technology has created several engineering and scientific opportunities, as well as related challenges. This requires increased research efforts from a variety of sectors including academia, industry, and government. The combined efforts of these industries should inevitably result in the development of the new protocols, systems, and services that are desperately needed to meet the IoT's difficulties. Recognizing the advancements in IoT technology and future applications, we set out to investigate the benefits, drawbacks, possibilities, and challenges that IoT technology, protocols, and applications bring. We have chosen a large number of research papers, and this article primarily outlines and provides an overview of the life-changing phenomenon of the Internet of Things, as well as the various technologies, challenges, and real-world applications that it has spawned, which have revolutionized our world with its wide-ranging outlook. This document also synthesizes existing knowledge and identifies common threads and gaps that open up new and demanding future research possibilities for IoT systems. In addition, various perspectives around IoT systems taking into account the relevance of security, privacy, and quality of service (QoS) concerns in the IoT industry are highlighted. Finally, this article summarises the available research and shows how it contributes to various areas relevant to the Internet of Things.

Motivation, Objectives, and Contributions

The remarkable recent developments in IoT technology have provided the opportunity to broadly deploy tiny sensors for wireless communication for various applications such as smart homes, smart cities, smart healthcare, and the smart industry [13]. The motivation behind this contribution is that in critical situations, IoT devices can effectively deliver highly secure information, less power consumption, and low-cost solutions to the wireless network. Given these exciting prospects for IoT, several technical challenges need to be tackled and used effectively for each specific IoT application [14]. The principal contributions in this paper are:

- To clarify IoT vision and definitions and to provide a comprehensive overview of IoT features
- To elaborate on the various IoT architectures, and protocols that result from the integration of IoT with different technologies
- Designing a technical taxonomy to classify the various IoT applications
- To provide a discussion about open IoT issues and challenges in IoT applications.

The paper is structured as follows: Section 2 provides the required background and related work. Section 3 details IoT architecture such as electronic tools, cameras, actuators, radio frequency identification devices ZigBee, Bluetooth, CC, networking technologies, near-field communication, etc. IoT applications are discussed in Section 4. Section 5 describes recent IoT protocols like MQTT, CoAP, RPL, etc. Section 6 discusses the key challenges of IoT, and Section 7 describes future directions. Finally, the article is concluded in Section 8. Moreover, the outline of the paper is illustrated as shown in Figure 2.



Section 1: Introduction	•Introduction of IoT.
Section 2: Literature Survey	•Discuss the required background and related work.
Section 3: IoT Architectures	•Addressed diffirent IoT architecture with diffirent layer.
Section 4: IoT Applications	•Discuss Applications of IoT in difffirent domain.
Section 5: IoT Communication Protocols	•Describes the recent IoT protocols like MQTT, CoAP, RPL, etc.
Section 6: IoT Challenges	•Discusses the key challenge of IoT
Section 7: Future Direction	•Describes the future direction.
Section 8: Conclusion	•Sum up of the paper.

Figure 2. Outline of the paper.

2. Literature Survey

This paper reviews the state of the art in the area of IoT, defining the concept and emphasizing its key contributions and shortcomings for each of the research papers reviewed here. The majority of authors describe the IoT in terms of unique aspects and interests such as security, privacy, healthcare, energy, etc. Here, the different approaches to these issue that have resulted in different IoT visions for future research are discussed.

Xu et al. [15] addressed the latest IoT situation and some of the technologies and industry-specific implementations of IoT, as well as some traditional IoT protocols. Their paper discusses existing IoT science, major technologies supporting it, and significant industrial IoT implementations, and further describes technological developments and barriers to recognizing IoT growth in industries. A significant addition to this study document is that it thoroughly discusses new IoT developments in each sector. Alhamoud et al. [16] described a smart system for the development of energy-efficient intelligent home wireless sensors for protection purposes. They created a smart framework known as SMARTENERGY.KOM for the energy-efficient smart home system. Akkaya et al. [17] proposed the name of the system, including an IoT-camera RFID tag and a PIR (proximity infra-red) tracker to establish an intelligent system in a smart house. Within their article, the framework for additional work is defined in order to build up fluent knowledge acquired from at least one of the numerous IoT tools, such as some temperature sensors, recognition cameras, and RFID labels, now available for use in such systems. The most recent situation utilizing a protocol for data transfer between two organizations and the way data can be handled using such a protocol is explored and explained by Andrea et al. [18]. They provided a detailed analysis of urban IoT infrastructure, protocols, and architecture. The same paper also addresses the technological approaches implemented in the smart city project of Padova, Italy, to provide details of IoT implementation in the municipality of Padova. In this way, the work can also be introduced and debated in conjunction with the municipality.

Al-Fuqaha et al. [19] addressed IoT interfaces and protocols for handling machine-to-machine contact between two systems without interrupting human beings, and identified some significant technology uses for IoT implementation and design. Their paper provides an overview of the IoT focused on technology capabilities, protocols, and implementation problems. It is through RFID, intelligent cameras, networking systems, and Web protocols that the IoT is enabled. According to Abdur et al. [20], as the number of internet applications used around the world increases, the field of life and action in day-to-day existence will shift in the future at a certain stage. If the IoT system happens as envisioned, 70 percent of devices will be targeted for protection. This additionally aims at a health concept for businesses, medical equipment, smart homes, and various IoT concepts, and provides an e-mail and SMS system that is focused on travel exploration. Raja et al. [21] have spoken about the Raspberry Pi being used in python material. A protection warning program is mentioned here that records a video when a motion is identified, loads it to the outside server, and notifies the consumer via text message. Tahir et al. [22] discussed Internet use and various forms of communication. Many different computers combine Wi-Fi, Bluetooth, and other features. They also discuss repetitive attacks in the same article. To resist internal attacks from malicious nodes, Wang et al. [23] proposed an ant colony optimization algorithm for secured routing based on a trust-sensing model (ACOSR) in wireless sensor networks. The simulation results show that the proposed algorithm has evaluated the efficiency significantly in terms of packet loss rate, end-to-end delay, efficiency, and energy usage, and demonstrate strong resistance to black hole attacks.

According to Zhu et al. [24], cameras are used for image recognition when recognizing an object in real-time. In addition, the system's deploying configuration is depicted, allowing for a simple security monitoring system to be established. Suchitra et al. [25] addressed the different protection requirements and issues of the IoT and analyzed the work of researchers who have previously identified this issue. Their paper explores the concept of a Denial of Service (DoS) attack. Zhang et al. [26] created a medical health monitoring device with the aid of a CC2430 microcontroller, a human information sensor, and microelectronic and modern wireless communication technologies. In addition to collecting medical signals, a sensor node circuit and a coordinator node circuit were planned, and wireless sensor network software was developed. Finally, each device module's online debugging was combined with hardware and software. The results of this experiment showed that the network node was trustworthy and that data transmission was precise. Wang et al. [27] suggested an anonymous batch handover authentication protocol that pre-distributes handover keys using a group signature technique. Unlike current group signature protocols, the proposed protocol avoids group signature correlation operations during the handover authentication process, resulting in improved performance. Afanasyev et al. [28] presented a detailed description of the principles and problems of the robotic internet of robotic things (IoRT) and suggested software for the IoRT. In their article, they state an intention to take further action in order to broaden the discussion regarding developing this interdisciplinary area. The same work analyzes possible solutions for the network of robotic things, discussing concerns relating to IoRT design, smart space incorporation, and robotic applications.

Dharshini et al. [29] addressed the application of IEEE 802.15.6 protocols, transmitters, and receivers. They also offer a brief overview of WBAN's sensor architecture, implementations, power efficiency, energy conservation, communication protocols, and security concerns. Alezabi et al. [30] introduced authentication and re-authentication protocols for 4G wireless networks, specifically LTE-Advanced (LTE-A) and WLAN, an interworking architecture, for 4G wireless networks. The protocols suggested are suitable for 5G networks. A new set of authentication and re-authentication protocols has been reinvented to provide quick and reliable handovers (HO) in current 4G and next 5G networks, taking into account existing standard authentication protocols. Weber [31] focused on global security and privacy issues and explored privacy and security challenges before mounting the IoT framework to work. In Edge-of-Things (EoT) applications, Toor et al. [32] implemented a dynamic speed scaling method. The proposed solution is thoroughly examined, with verification obtained through simulations performed on the iFogSim simulator. The results show that dynamically scaling the processor frequency of EoT devices in response to load variations in IoT traffic significantly improves energy conservation. Liu et al. [33] proposed a verification system with clarification to determine confirmation and access control based on an elliptical curve cryptosystem, and established it on diverse security threats. Huang et al. [34] explored how to achieve physical layer-protected connectivity by forming virtual beamforming through the collaboration of jamming nodes to point to hostile wiretap nodes. The simulation results show that power dynamic allocation and pricing have strong convergence, and the source node offers a train of thought for selecting cooperative nodes and their number.

Li et al. [35] discussed the heterogeneous nature of IoT objects and devices and ways that IoT researchers and developers are actively engaged in developing solutions for problems. Pierleoni et al. [36] introduced an IoT architecture for building monitoring that is continuous and real-time. The proposed method is based on a sensor node located inside the monitored building that is connected to the Internet and capable of performing continuous measurements and sending raw data to a remote server via the MQTT protocol in real-time. Luk et al. [37] addressed System Security Networking (SSN), recovery and privacy safety, and authentication. By combining first-order reasoning and probability graphic simulation, Li et al. [38] proposed a hybrid approach to complex everyday task identification. They created a novel "Markov logic network" that combines data-driven multi-feature modeling and inference with simpler rules-based modeling and inference, allowing and promoting the applicability and robustness of everyday activity recognition. A Delay and Energy-Efficient Data Collection (DEEDC) scheme, as discussed by Xiang et al. [39], employs a clustering approach. Matrix filling theory is used to quantify the number of slots available for transmission for each cluster, not the number of nodes that produce data. This means that data can be obtained in a network of randomly distributed data (number of slots, number of nodes), preventing slot distribution and repetitive data acquisition, which wastes time and resources. Hussain et al. [40] reviewed the security criteria, attack vectors, and emerging security options for IoT networks in a comprehensive way. They then discuss the flaws in these security solutions, which necessitate the use of ML and DL techniques. Finally, they address the latest ML and DL solutions for solving various security issues in IoT networks in depth.

A bit error performance evaluation of chaotic sequences was presented by Novosel et al. [41]. For USRP software-defined radio, the performance of chaotic sequences is evaluated using multiple access spread spectrum system models. Numerical simulations and bit error rate analysis are performed using LabVIEW. One-dimensional, two-dimensional, and three-dimensional maps are used to create chaotic sequences of various lengths. To reduce the delay for Industrial Internet of Things (IIoTs), Wu et al. [42] suggested a Learning-Based Synchronous (LS) method from forwarding nodes. When using an asynchronous Media Access Control protocol, senders must always wait for their corresponding receiver to wake up before sending results. As a result, the delay is longer than in a synchronous network. Stergiou et al. [43] proposed a revolutionary infrastructure for handling Big Data (BD) on smart buildings that run on a wireless-mobile Sixth-Generation (6G) network. When the telecommunications industry expands, new threats emerge. Furthermore, a new form of wireless network technology, known as 6G, offers all of the advantages of previous generations while addressing some of the problems that have plagued its predecessors. Temglit et al. [44] proposed QoS and the establishment of IoT hardware, events, and administrations as a major basis for gaining consumer trust in IoT administration and hardware, as there are substantial problems and companies can be volatile. Wan et al. [45] proposed a novel framework for real-time personal health tracking called the Wearable IoT Cloud-Based Health Monitoring System (WISE). To enable real-time health tracking, WISE uses the BASN (body area sensor network) platform. Sensors for heartbeat, body temperature, and blood pressure sensors are among the wearable sensors that have been embedded.

In a high-frequency structure simulator, Ali et al. [46] developed a multilayer model of the human head and hand. They calculated the effects of the unique absorption rate by simulating antennas equipped with the head and hand models in the final stage. The antennas were placed on the built model to measure the specific absorption rate for the head and hand. Liu et al. [47] proposed a smart 5G IoT network based on ambient backscatter communication. The network is made up of two parts, a real-time data transmission system that uses ambient backscatter communication, and a real-time big data processing system that uses a mixture of shallow and deep neural networks. Majeed et al. [48] used previously neglected unmanned aerial vehicle (UAV) energy consumption parameters to determine the current state of available energy, and suggested a solution that more reliably estimates UAV operating airtime. The proposed model was tested in a test bed and a simulation setting; the results show that taking into account such explicit utilisation parameters improves airtime estimation significantly. Jebarani et al. [49] proposed a framework that includes medical data being transferred through the Remote Human Health Care Model. A low-energy adaptive clustering model was used to build the data transmission model. Raji et al. [50] compared the wavelet transform of output to potential wireless application framework specifications and proposed wavelet implementations in 5G waveform architecture guidance and approaches.

Palattella et al. [51] discussed security and privacy, describing security issues that will be addressed by future technology. They state that the key test in the years to come will incorporate both basic determination of advancements to handle the many open issues and a push to pass these plans on to authentication structures and applications. By considering both the technical and standardization dimensions, they examine in depth the potential of 5th Generation (5G) technology for the present IoT, and discuss the existing IoT networking environment as well as the key IoT 5G enablers. Kaur et al. [52] proposed an information model to record and utilize IoT information, and discussed use cases emerging across China and different nations and areas in connection with the COVID-19 pandemic. Their paper provides insight into the flow of examining inclines as well as some future research bearings. Behera et al. [53] proposed a wireless sensor network for use in their research scenario, and described how such a network can manage the battery for increased lifetime as well as how cluster head cells are activated for data aggregation and network efficiency enhancement using the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol. Farman et al. [54] discussed the LEACH protocol and a modification of the LEACH protocol to provide efficient use of power, resulting in improved network efficiency at a good ratio. Behera et al. [55] proposed an enhanced version of the LEACH protocol so that the network can be used for different applications. With the use of the clustering head technique and with the help of a single cluster head, network performance can be improved. Butler et al. [56] proposed an IoT architecture in which different IoT devices can sense data and aggregate it for different environments. L. Hu et al. [57] discussed smart cloud use in the IoT network to increase data storage capacity; for training using this method, they relied on a sensor-based cloud system.

Alzahrani et al. [58] discussed a survey on patient physical healthcare monitoring and authentication protocols designed for the WBAN environment. Although this was an efficient scheme for employing lightweight operations, the paper reveals some security loopholes. This framework was limited to security features, not energy efficiency. Wang et al. [59] highlighted the ways in which data storage generated by many sensor nodes represents the biggest challenge in the IoT network. They described an efficient computing technique that reduces power consumption and increases the storage capacity of the network. Qi et al. [60] discussed malicious IoT nodes and the effect these have on future IoT networks. Because of this challenge, they expanded the current Locality-Sensitive Hashing (LSH) methodology to incorporate the time factor and further introduced a new LSH-based approach to time-aware and privacy-conserving service recommendations. In order to confirm the feasibility and efficiency of this proposal, they performed detailed experiments on a large-scale real-world dataset. The results of the experiment show that in guaranteeing privacy preservation, the method achieves a successful trade-off between accuracy and efficacy of recommendations.

Yang et al. [61] proposed a blockchain in the IoT network that works as a centralized server to control and manage IoT networks. Their simulation results show that the proposed device is efficient and feasible for capturing, measuring, and storing trust values of in-vehicle networks. Marche et al. [62] focused on modeling the trustor–trustee relationship in the Internet of Things and proposing recommendations for designing trust management models effectively. The effects of the proposed guidelines on a basic confidence paradigm were shown by simulations. Wang et al. [63] discussed Mobile Edge Nodes (MENs) and also described edge techniques to reduce power consumption and enhance the performance of the network. Khraisat et al. [64] proposed a novel IoT intrusion detection system (IDS) taxonomy that illuminates IoT IDS techniques, their benefits and drawbacks, IoT attacks that target IoT communication networks, and the related advanced IDS and detection capabilities to detect IoT attacks. This technique, called "cluster head," gathers information from neighboring nodes and then aggregates it so that power can be reduced for the performance enhancement of the IoT network. Haris et al. [65] proposed the use of IoT networks for 5G technology and also discussed how 5G technologies can be advanced with IoT sensor nodes. The concept of the CPS was introduced with the IoT structure. Srivastava et al. [66] discussed the energy-saving protocol used in WSNs and provide a comparative analysis of multi-agent and single-agent-based protocols. In a 5G IoT scenario involving several UAVs, Fu et al. [67] addressed the connectivity issue between UAVs and cellular base stations; these are responsible for uplink channel modeling and uplink transmission efficiency analysis. They also consider the effects of 3D distance and multi-UAV reflection on wireless signal transmission in the channel model. Yi et al. [68] established a safe energy exchange network. In comparison to other related schemes, the blockchain-based energy sharing IoT framework offers more stable consumer services. Furthermore, such technology can help secure user privacy. Gulzar et al. [69] discussed climate-smart agriculture to reduce the many losses due to climate effects. In addition, they provide a review of agricultural literature related to IoT design.

Anwer et al. [70] discussed cryptography algorithms for the IoT network with the help of blockchain technology to provide a secure flow of information between sensor nodes. Mughal et al. [71] proposed a cellular architecture whereby IoDs utilize the resources of the cellular network for energy harvesting and information transmission. The radio resources of the cellular network are divided by time and frequency, and each time-frequency block is called a Cellular Resource Block (CRB). To verify the derived analytical expressions, system-level simulations were carried out showing that the analytical results matched the simulation results. Moreover, the overall performance of the considered architecture was studied for different system parameters. With the support of an IPv6 over Low Power Wireless Personal Area Networks Protocol (6LoWPAN), Jose et al. in [72], discussed the protection features of the IoT network and also suggested a definition of an IoT scenario RPL protocol. Their paper discusses the routing needs of a Low-Power and Lossy Network (LLN), the original protocols, and new approaches. The enhancements to IoT routing are divided by their core goals and then analysed separately for their major strengths and limitations. Another key contribution of their review is its overview of considered solutions, discussion of open problems, and suggestions for new future ideas. Jangid et al. [73] discussed the risks and security problems in IoT-based devices used in healthcare systems. Cyber-protective threats remain present with both physical and mobile devices; robots are often affected by cyber-safety threats, and hackers can exploit contact between robots and surgeons. Apart from the above study, Table 1 provides IoT-based research topics along with a literature pool. Although IoT is, of course, considered a boon, because it is linked to the Internet networked devices are susceptible to security threats.

Table 1. IoT-based research topics related with literature pool.

Research Area	Research Topics and Literature Pool	Specific Concepts Covered
IoT Standardization	IoT framework [15,18,67,68]	IoT concept, construction of protocols, standardization of architecture, vision, and system creation.
IoT System Architecture	Conceptual models [28,30,36,45,46,64] Hardware architectures [56]	System infrastructure, cloud-centric, workflow design, and concept templates.
IoT Interoperability and Integration	General interoperability issues [35,39,47–49] Gateway's support [57,58]	General questions, architecture and IoT platforms, technical and semantic, Interoperability.
IoT Scalability	Massive scaling issues [21,24] Discovery service for the IoT [72]	Scaling of problems on large networks and sites, future exploration tools.
IoT Management and Self-configuration	Devices management [21,54] Network management [55,61] Applications and data management [62,63,65]	Control and management of the IoT layer, tools, network, software, data, and confidence.
IoT Identification and Unique Identity	IoT and IPv6 integration [25,32,73] Services discovery protocols [34,38]	Discuss challenges and approaches, internet protocol IoT incorporation, authentication, and authentication problems.
IoT Power and Energy Consumption	Low-power communications [16,29,50,53] Low-power chipsets and terminals [59,66]	Energy-efficient regulation and management of computers and chips.
IoT Security and Privacy	Security issues [17,20,22,23,26,27,31,33,37,52,60,70]	Problems with protection and privacy, concept and architecture of secure IoT networks.
IoT Environmental Issues	Green IoT technologies [19,40–42,44,69]	Environmental technology participation in IoT architecture.

Large corporations and cyber-security experts are getting better at addressing these concerns, but there is always room for improvement. The IoT design agency claims that development should go beyond architecture and incorporate all IoT modules in a manner that concentrates on compatibility, analysis, and precision at all levels while retaining the potential to enhance the practical performance of a product or service and effectively focus on new technologies.

Table 2 provides a comparative study of various reported works on the state of the art in the field of IoT, along with their major research directions. The concept of IoT has attracted considerable research attention, as the massive connectivity it promises brings with it a variety of challenges and research gaps including heterogeneity, scalability, security, privacy, data management, interoperability, standardization of energy needs, etc. This work aims to provide a succinct overview of IoT concepts and applications and to explain key components and features. This paper discusses a large number of research papers, and primarily outlines and provides an overview of the life-changing phenomenon of the Internet of Things as well as the various technologies, challenges, and real-world applications it has spawned which have revolutionised our world with this wide-ranging outlook.

Table 2. Comparative study of various reported work on the state of the art in the IoT field, with research directions.

Research Work	Major Research Direction	Evaluation Parameter				
		RT	RL	AV	CT	EC
Alhamoud et al. [16]	Energy, data processing	-	x	X	x	-
Zanella et al. [18]	Smart city, transport, and healthcare	x	-	X	x	-
Dharshini et al. [29]	Environment, power, and energy smart	x	-	X	x	x
Alezabi et al. [30]	City, transport, and healthcare	x	-	X	x	x
R.H. Weber [31]	Security and privacy	x	x	-	x	x
Li et al. [35]	Security and privacy, reliability	x	x	X	-	-
Pierleoni et al. [36]	Aggregation, Security, and privacy	-	x	X	-	-
Luk et al. [37]	Security and privacy, architecture	x	x	X	-	-
Xiang et al. [39]	Interoperability, QoS, scalability	-	-	X	x	
Wu et al. [42]	Security, agriculture, environmental	x	x	-	-	x
Stergiou et al. [43]	Data processing environmental	x	x	X	-	-
Temglit et al. [44]	QoS	-	x	X	-	-
Majeed et al. [48]	Environment, interoperability, scalability	x	-	-	-	x
Jebarani et al. [49]	Environment, interoperability, reliability	x	x	X	-	x
Raji et al. [50]	Energy, scalability	x	x	X	-	x
Palattella et al. [51]	Interoperability, reliability, scalability	x	-	X	-	x
Trupti et al. [53]	Energy, aggregation, and Throughput	-	x	-	x	-
Khraisat et al. [64]	Security and privacy, data processing	x	x	X	-	x
Anwar et al. [70]	Standardization, authentication, and identification	-	x	X	-	-
Jangid et al. [73]	Security and privacy	x	x	X	-	x

Terms Used: AV: availability, CT: cost, EC: energy consumption, RT: response time, RL: reliability.

3. IoT Architectures

There is no single universally agreed-upon consensus on IoT architecture. Different architectures such as healthcare-based architecture, smart home-based architecture, and FC-based architecture, etc. have been proposed by different researchers.

3.1. IoT General Architecture

The IoT area includes a wide variety of technologies based on different architectures. Thus, it is impossible to use a single reference architecture as a blueprint for all possible concrete implementations. While it is understood that a specific paradigm occurs, other similar models will coexist on the internet. In this context, the architecture is specifically defined as a framework for the description of the physical components, functional arrangement, networking, operational principles, procedures and data formats used in its operation [74]. The IoT design of patented protocols is extremely scalable and can support several different network implementations, as seen in Figure 3. In order to facilitate internet integration in the data environment, certain middleware should also be included for scalability, stability and semantics. Several different physical objects, devices, application networks, engineers, activators, networking channels, customers, market rates and IoT protocols are part of the IoT framework; the IoT layer architecture is shown in Figure 4. It mainly functions on three layers; the function of each layer is discussed below.

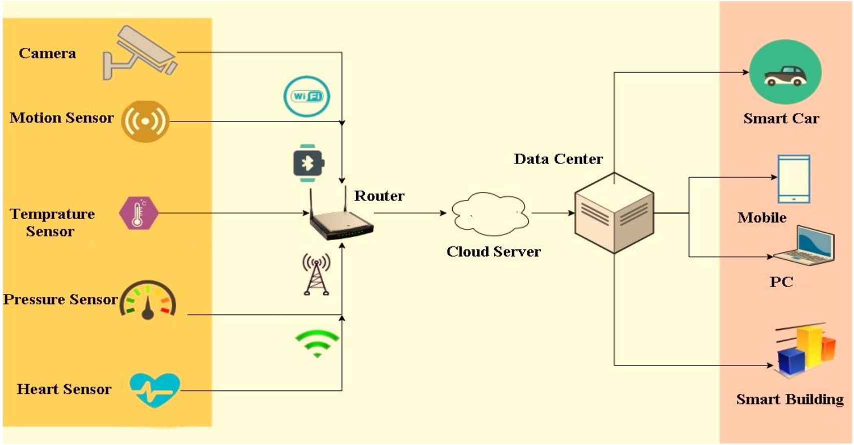


Figure 3. IoT Architecture.

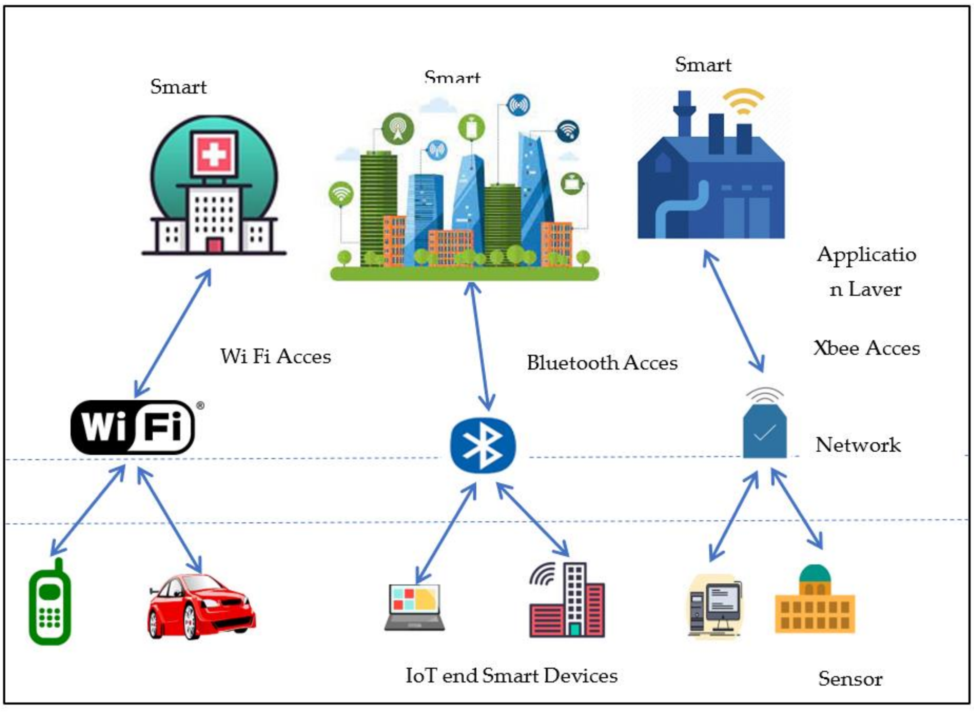


Figure 4. IoT layer architecture.

3.1.1. Perception Layer

The perception layer is also known as the physical layer, and directly works with IoT sensors. The interesting aspect of sensors is their capacity to interpret knowledge received from the outside environment. In other words, in order to continue to include of sensors in the three stages of an IoT architecture system, it is necessary to get information in a format that can be processed. The exceptional feature of sensors is the ability to convert data obtained from the outside world into analysis. In other words, the incorporation of sensors into the three stages of the IoT system background will begin to include details with a look and feel that can be easily interpreted. The cycle continues with actuators, which are capable of interacting with physical realities. For starters, a light may be switched off, or the temperature in a room changed. As a consequence, the sensing and operating stages cover and change anything required for additional study of the real environment.

3.1.2. Network Layer

The network layer provides the network with access to the data, and works as a cloud. The network layer links to other intelligent objects, network appliances and servers. Its capability is often used for the transfer of sensor data and analysis. The optimised details are passed to the IT environment during this period through the phases of the IoT architecture. Enhanced analytics and preprocessing are carried out by edge IT systems, in particular; this applies to, for example, the technologies of machine learning and visualization. Around the same point, any extra testing will happen in the data center. In addition, stage two is similarly related to the previous phases of IoT construction. It ensures that the edge IT systems are placed next to those where the sensors and actuators are installed, and that a wiring closet is built. At the same time, it is also necessary to live far from the workplace.

3.1.3. Application Layer

The application layer provides unique consumer resources. It describes different applications for IoT such as smart houses, intelligent communities, and intelligent well-being. Throughout the data center or cloud, the core processes exist in the latest phase in the IoT architecture. This enables detailed treatment, and a follow-up review of feedback in particular. The expertise of IT and Operative Technology (OT) experts is needed here; that is, the process contains now the highly ranked scientific knowledge in both the modern environment and in humans. Data from other websites should also be used here in order to allow for a detailed review. Notwithstanding, the volume of information produced is becoming difficult to store and process in neighborhood stages. The adaptability offered by CC answers this issue. Distributed computing provides assets while requiring little to no effort on the part of clients.

3.2. IoHT Architecture

The main design challenges for an efficient IoT architecture in a heterogeneous setting are scalability, modularity, interoperability, and flexibility [75]. The IoT architecture must be built to fulfil the needs of cross-domain interactions, and multi-system integration, with the ability to provide easy and flexible functional management relations, massive data processing and storage, and user-friendly applications. The software should also be able to scale up its features and incorporate some insight and automation into the system's IoT computers. The amount of massive data produced by the communication between IoT sensors and devices represents a new task. Therefore, the large volume of streaming data in the IoT framework requires a powerful architecture. Perception, network, and application all operate on three different levels.

Figure 5, based on IoHT, portrays the information stream across these layers. Because of human association, each layer in [46] has certain security issues, including secrecy, honesty, and credibility. The human connection has raised affectability; therefore, information acquired from people and patients requires authorization from the framework in order to acquire to the data. Due to protection concerns, clients are unable to completely utilise some gadgets. Medical care information assurance is basic; along these lines, information realness, genuineness, and classification should be maintained. For the ongoing wellbeing check framework, it is necessary to construct a security system. Health technicians and paramedics now use a variety of protection frameworks and equipment.

3.3. IoT Architecture with FC

FC data is obtained from sensors connected to physical devices in an IoT platform. The FC model uses local computing services located at the network edge rather than CC resources. Low latency, real-time decisionmaking and optimum bandwidth usage are some of the key advantages of this paradigm. The FC architecture enables fog nodes, cloud, and IoT to be moved dynamically through processing, networking and storage services. However, fog interfaces may enable the versatile and complex movement of devices, storage, and control roles between these various organizations to communicate with the server, other fogs, and staff or users. This has facilitated well-located FC consumer evaluation and has also allowed accurate and successful control of QoS. FC acts as a cloud-to-end gateway that enables end-users to access data, storage, and network resources. The nodes of fog are referred to as such units. They can be mounted anywhere with a network connection. Figure 6, based on the optimization of QoS parameters and the proposed model, illustrates the smart city technology architecture of the new platform. The functions of the different layers are explained below.

3.3.1. Cloud Computing

Cloud computing and stacking the CC layer is responsible for compiling and executing information derived from other layers in heterogeneous IoT. CC with a diverse set of heterogeneous IoTs is able to handle the massive volume of data immediately and in a particular manner. Because cloud services can track hierarchical computing, this is likely. In addition to storage capacity, cloud providers also can make decisions based on the information obtained. In addition, relying on emergency event-aware architectures, cloud vendors can take decisive action in certain critical heterogeneous IoT environments.

3.3.2. Fog Layer

The conceptual fog manager is in charge of this layer, which analyses and categorizes requests based on their complexity at the time. The fog handler is a critical component for optimizing QoS and tool use on fog layers.

3.3.3. Sensor or Physical Layer

Specific sensors in the IoT's physical layer collect data from different locations which are then fed into the cloud infrastructure for decision-making. A large number of sensors are placed in a specific location, and a topology is developed for data transmission. In a standard network, there are sink nodes, sensor nodes, and control nodes.

Fog nodes act as a bridge between the end device and the cloud infrastructure. The fog nodes are considered transient and consequently not trusted. The end device (for example, a user or an IoT smart device) must be authenticated by the fog node before any service is provided. This authentication can involve the cloud server, which introduces latency as well as overhead at the cloud server. Normally, authentication and session key establishment between an end device and the fog nodes relies on public-key cryptography. However, this is rather computationally expensive, relatively speaking. Fog nodes are considered transient possibly due to the nodes being out of range or becoming offline for various reasons. In this case, the end-user will need to re-authenticate with a secondary fog node that will take over the prior fog node's job. The primary goal of this research is to accomplish failover re-authentication without the need for public-key cryptography. This may be accomplished if the fog nodes agree on some security tokens ahead of time which are then made available to the end device after the first authentication. These security tokens may be used to provide quick authentication between the end device and the secondary fog node. Furthermore, unsecured communication between end devices and fog nodes can expose an adversary to a variety of security attacks such as replay, impersonation, man-in-the-middle, and denial of service attacks.

3.4. IoT Architecture for Smart Homes

A sensor creates data, but it contributes little value to the home environment on its own. A thermostat is often not called “smart” because the homeowner must regulate the temperature based on the outside temperature, humidity, and other factors. It is possible to maintain a stable temperature, but this is automation, not “smartness.” Only when all environmental data is collectively analysed based on collected patterns and decisions made without the intervention of the consumer can it be called a “smart” ecosystem. The way sensors interact, how and where sensor and equipment usage pattern information is processed, how this data is interpreted and patterns are detected, and how the systems can be interacted with by the consumer and vice versa is decided by the smart home infrastructure.

The symbiosis of numerous components, such as sensors, connections, and applications, that generate a complex, heterogeneous infrastructure to effectively control home devices and provide advanced services to consumers can be described as a smart home. Figure 7 depicts cloud-based smart home architecture in general. The internal network consists of terminal equipment, cameras, processors, and actuators. These machines link with a firewall at the network’s edge, which makes linking internal networks to the internet even simpler. The communication difference between end-users, sensors, software, and the cloud is bridged by a gateway computer [76].

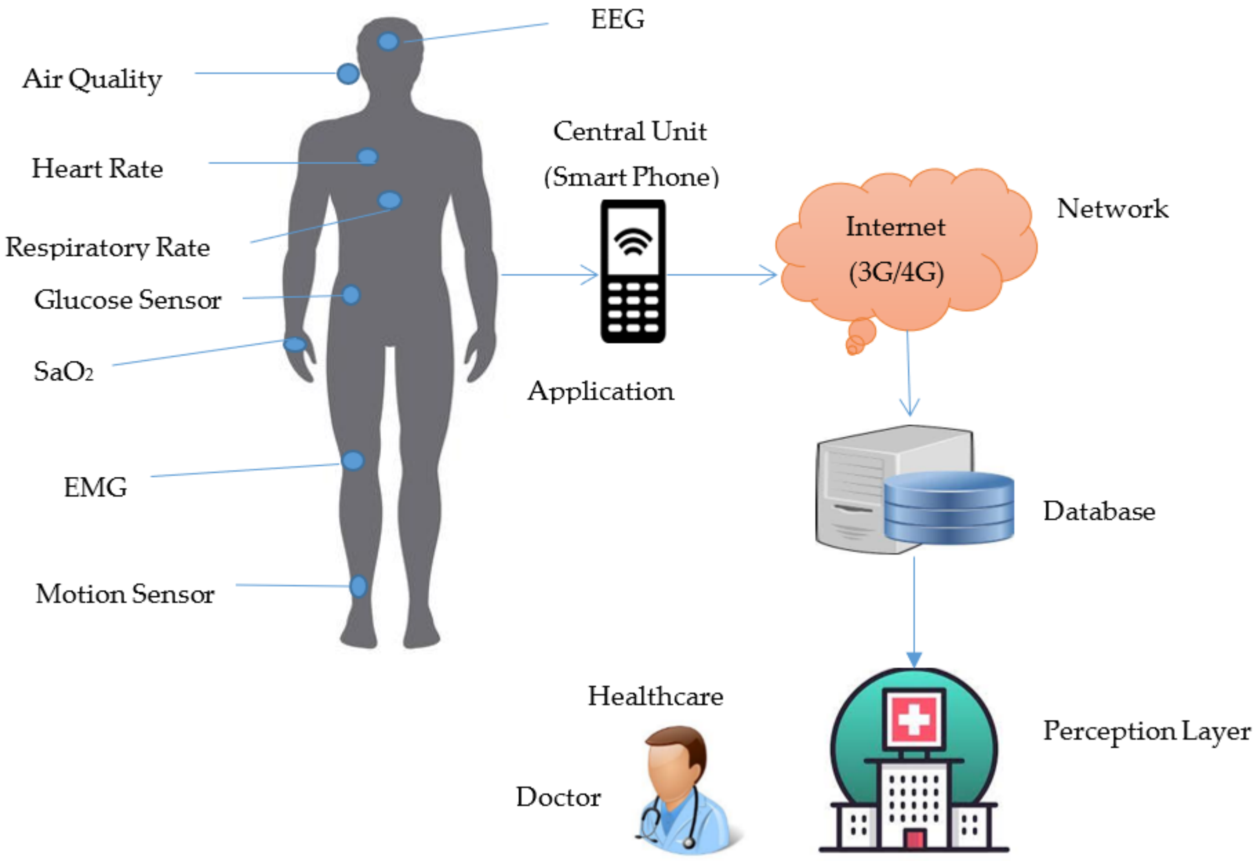


Figure 5. Healthcare models of IoHT.

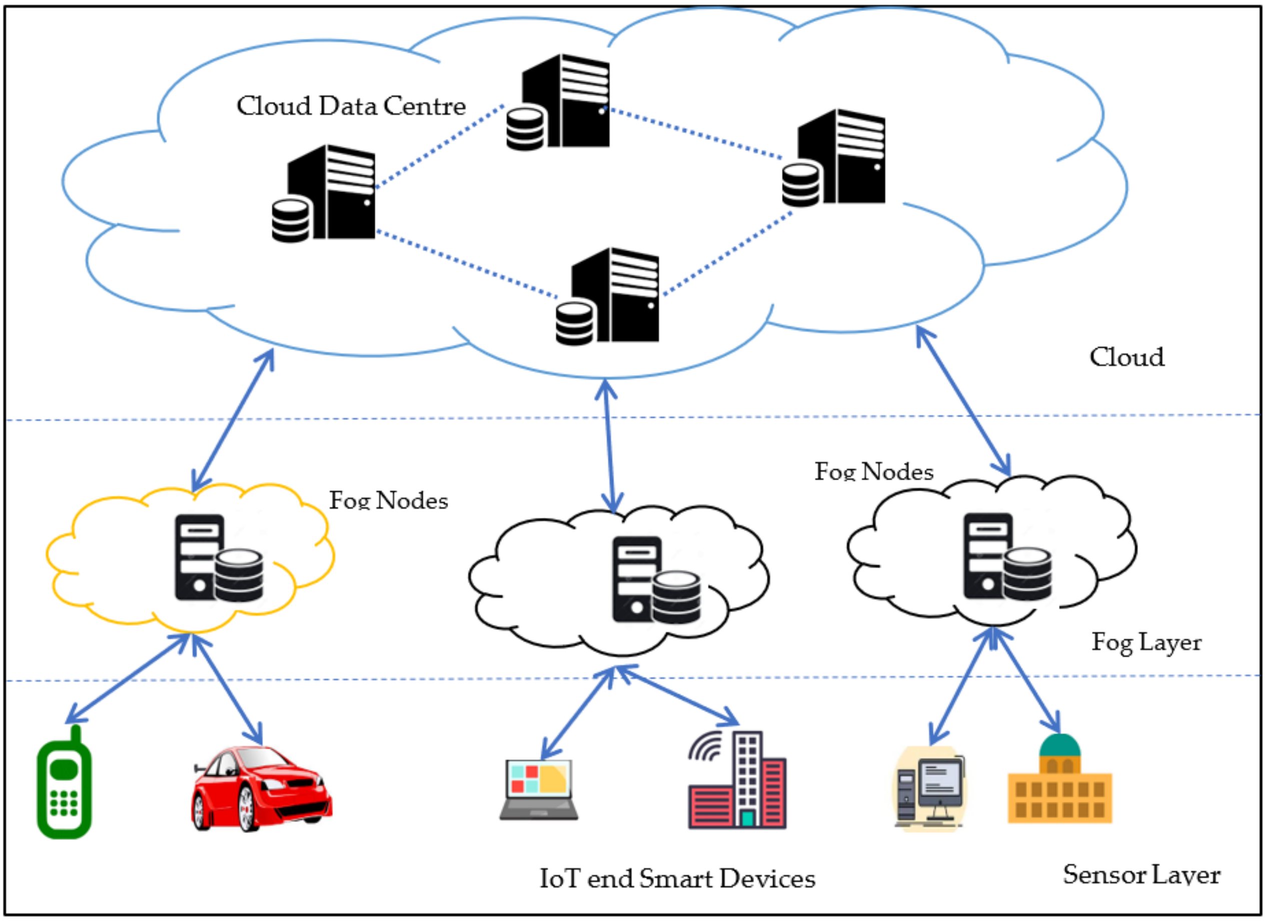


Figure 6. The system architecture of IoT with fog computing.

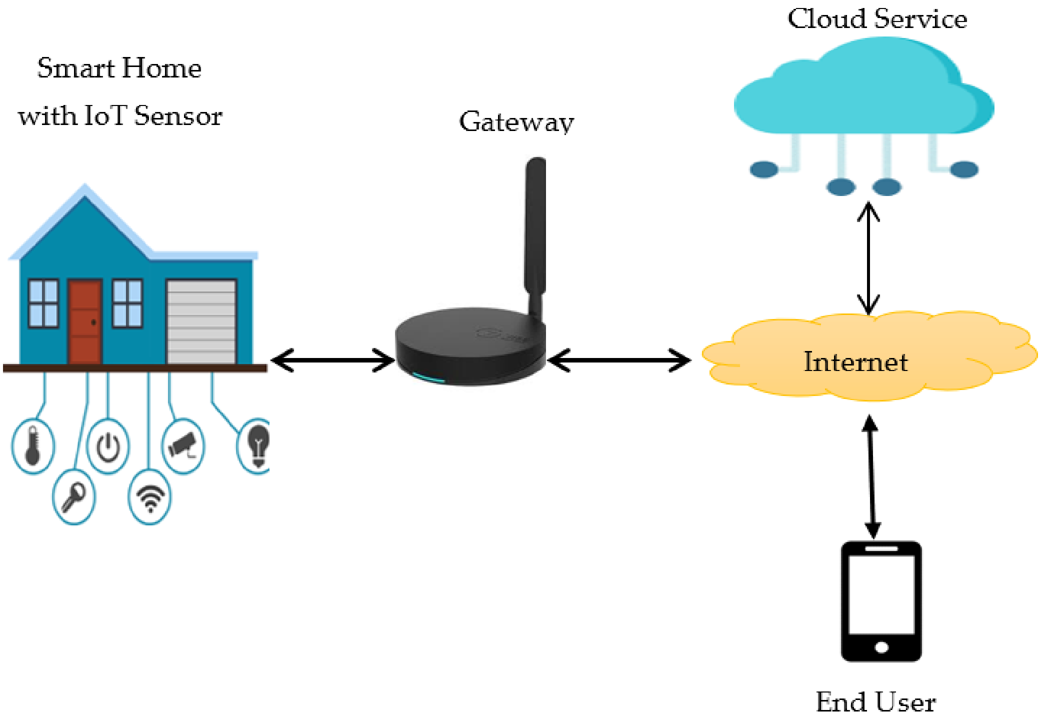


Figure 7. IoT-based smart home architecture.

A smart home gateway architecture that is configured in terms of accepted communication protocols and can convert heterogeneous data from sensors into a standard format. In general, the gateway is a device that accepts several communication protocols with the end devices for interoperability. It is efficient enough to do any computation at the edge of the network before uploading the data to the cloud. The gateway further adds a layer of security to the smart home network as it connects contact between end devices and the outside world, meaning all communication is filtered before instructions are transmitted to the end devices. This effectively includes ways to improve usability, stability and security while at the same time taking advantage of higher computational power and scalable architecture. The cloud can connect multiple services from third parties as well, such as data visualization, control of smart home products, or access and role management for consumers.

3.5. Blockchain-Based Smart City Architecture

Blockchains are decentralised distributed ledgers, a game-changing technology that may help solve IoT security issues. A blockchain-based approach to IoT networks might address many of the issues with the existing paradigm while also increasing security. The use of blockchains in IoT security allows for direct information exchange between connected devices rather than communicating through a centralised network, reducing the IoT's vulnerability to cyberattacks [76]. According to a Gartner report, healthcare, transportation, and energy have the greatest rates of blockchain use among IoT-enabled firms in the United States.

When it comes to encryption, the technology employed in digital ledger systems is rather advanced. Because a blockchain is an encrypted database that is distributed, decentralized, and impenetrable, it has sparked the minds of today's youth. Since its inception, it has been used to reshape the way business is done in nearly every area, spanning government, finance, healthcare, and smart cities. Figure 8 depicts a blockchain-based smart city architecture that includes different IoT devices and infrastructure applications. IoT device integration involves cloud systems, edge computing, gateways, and many types of IoT devices, ranging from basic sensors that can only communicate with adjacent gateways to devices with computational and processing capabilities. It is amazing to see how blockchain and edge computing are linked. Blockchain nodes can use edge computing or distributed computation architectures to store and validate transactions. On the other hand, blockchains can create a completely open and distributed cloud marketplace.

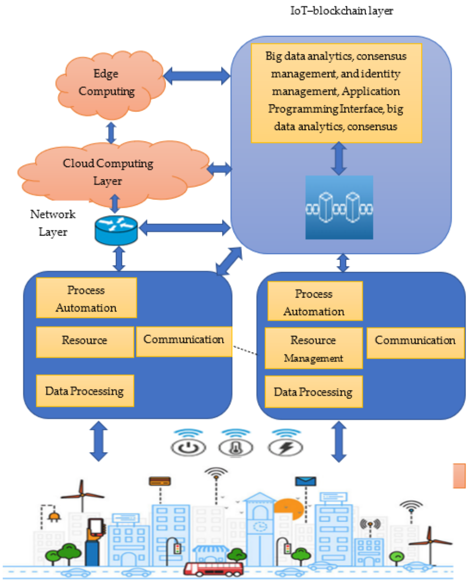


Figure 8. Blockchain-Based Smart City Architecture.

4. IoT Applications

IoT technologies pledge human lives to be of tremendous importance. IoT could be the next phase in the form of the wallet connecting modern cellular networks, superior devices, and innovative computational capabilities. IoT technologies are supposed to provide communication and information for trillions of daily items. The various application domains of IoT are shown in Figure 9.

4.1. Smart Home

Smart homes take care of problems such as activating environmental checks so that when a person comes into the house, it is already fully comfortable. Dinner that needs an oven or a crockpot may be prepared remotely so that the meal is ready immediately.

Protection devices are also rendered more available by allowing customers to remotely monitor appliances and lighting, and to activate the smart lock to enable appropriate individuals to enter the house even though they do not have a key [77]. Some smart home features are shown in Figure 10.

4.2. Smart Agriculture

The use of IoT in agriculture targets traditional agricultural practices to satisfy rising demands and reduce output losses. IoT utilizes robotics, drones, remote sensors, and computer vision in agricultural industries together with rapidly evolving machine-learning and analytical instruments for field observation, farm surveys, and monitoring, which provide farmers with knowledge regarding appropriate farm management strategies to save both time and energy. In indoor planting, IoT allows micro-climate monitoring and management, which effectively increases efficiency. For outdoor planting, soil humidity and nutrients can be sensed in conjunction with temperature to enable smart irrigation and fertilizer systems through devices using IoT technology. For instance, when water is provided only by sprinkler systems, this may prevent a useful resource for being lost [78]. Some smart agriculture features are shown in Figure 11.

4.3. Smart Cities

IoT can enable smart city technologies to spread through many industries, leading to a safer atmosphere and increasing public protection and road lighting. Intelligent parking systems can determine if parking lots are filled or open, and build intelligent community systems using GPS data from drivers' smartphones or ground-surface sensors installed on the floor on parking lots. As the name implies, intelligent cities are a major advance that includes a broad variety of use cases, from the delivery and control of water, to traffic, to waste reduction and environmental protection [79]. Some smart city features are shown in Figure 12.

4.4. Smart Health Care

In the first instance, wearable IoT technology allows hospitals to track the safety of their patients at home and thereby minimize medical visits while also delivering knowledge that can save lives in real time. For hospitals, intelligent beds can keep workers updated about the bed supply for more efficient use of rooms. Placing IoT captors on vital hardware ensures fewer faults and greater durability, which can make a life-or-death difference. Reactive medical networks will become adaptive, wellness-based devices with IoT implementations. Important real-world knowledge is scarce as a tool of modern medical science. It utilizes much of the available info, managed environments, and medical test volunteers. Through observing, utilizing real-time data, and evaluating, IoT opens a door to a world of usable data. IoT also increases the strength, efficiency, and usability of installed equipment. IoT is not only about hardware but also about building structures [80]. Some smart healthcare features are shown in Figure 13.

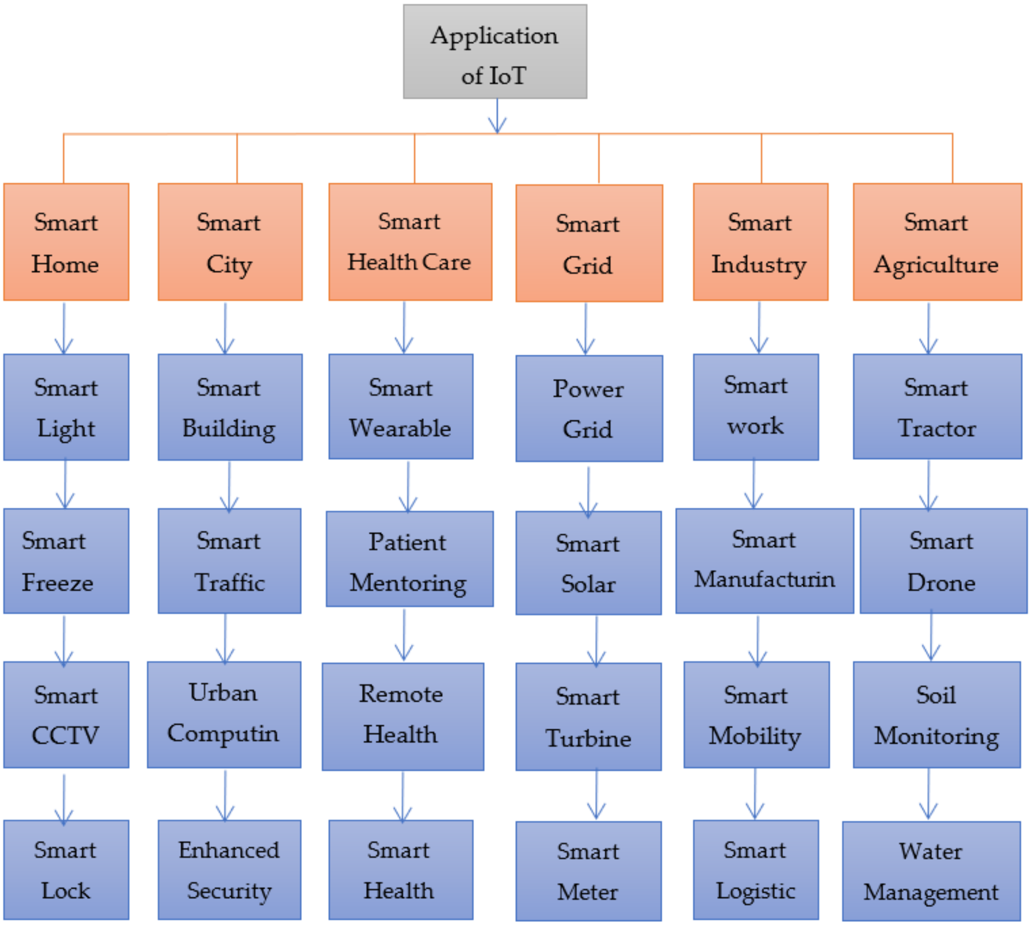


Figure 9. Application domains of IoT.

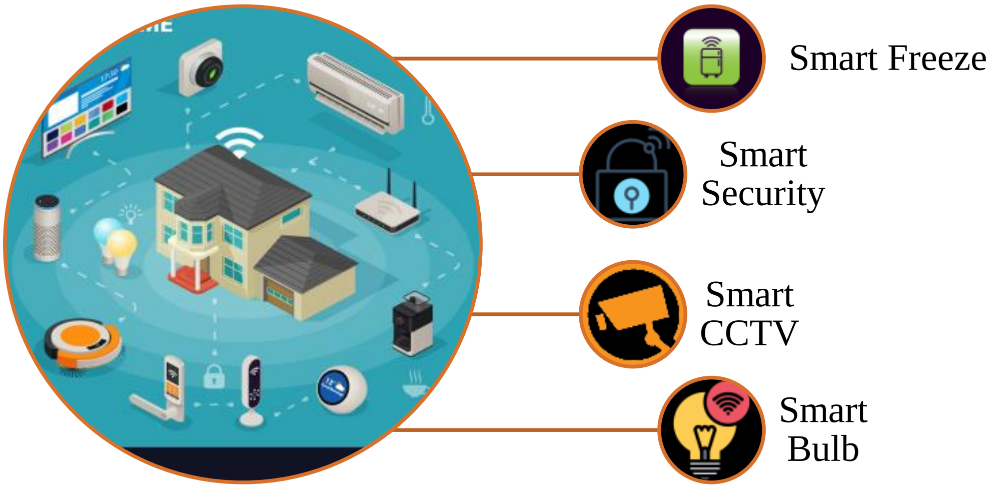


Figure 10. Smart home features.

4.5. Smart Grids

The interesting field is intelligent grids of IoT technologies. In turn, an intelligent grid aims to continuously collect knowledge from customers and power providers on the actions of energy supplies to boost the quality and reliability of delivery. IoT devices for tracking climate, such as moisture, temperature, and illumination, may be used. The IoT sensor knowledge will assist with the development of algorithms to monitor energy consumption and adapt accordingly, replacing the human factor [81]. Some smart grid features are shown in Figure 14.

Figure 11. Smart Agriculture Features.

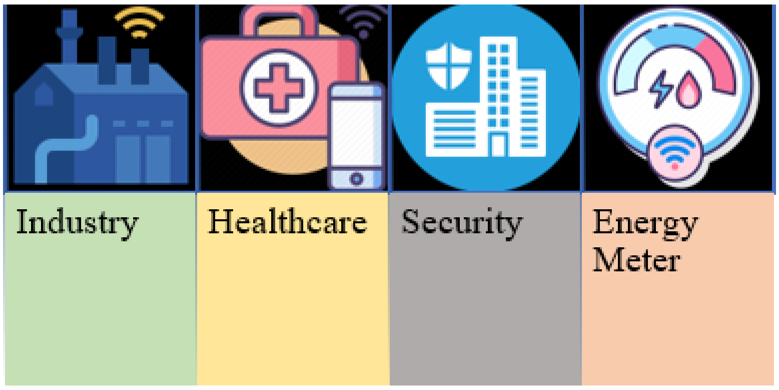


Figure 12. Smart city features.

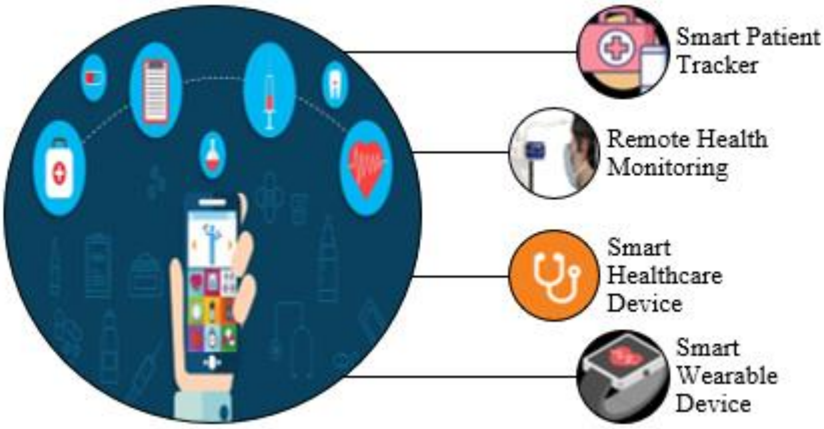


Figure 13. Smart health care.

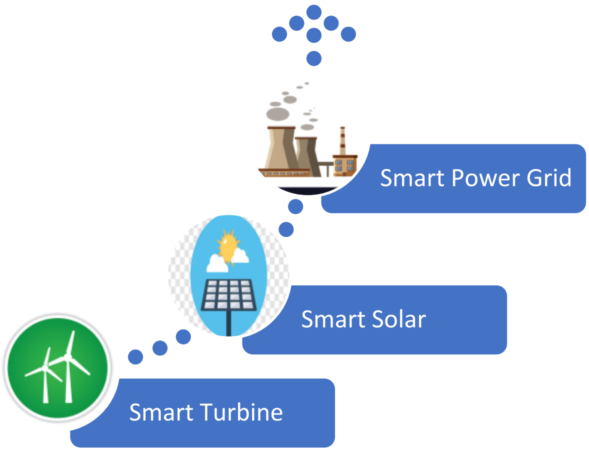


Figure 14. Smart grid features.

4.6. Smart Industry

Another way to learn about the Internet is to look at connected devices and equipment in sectors such as power production, mining, gas, and medical services. This also concerns circumstances in which unplanned disruption and faults in the network will contribute to life risks. A device installed in the IoT appears to provide devices such as cardiac tracking exercise bands or intelligent home appliances. Such programs are reliable and should be simple to use, but they are not efficient, because they usually struggle to establish emergencies. Another huge champion in the IoT sweepstakes is the automotive and industrial automation sector. From start to finish on the manufacturing floor, RFID and GPS systems can help a supplier monitor a commodity across the entire supply chain throughout its destination shop. Sensors may gather details about travel duration, the state of a device, and the environmental conditions of the system [81]. Some smart industry features are shown in Figure 15.

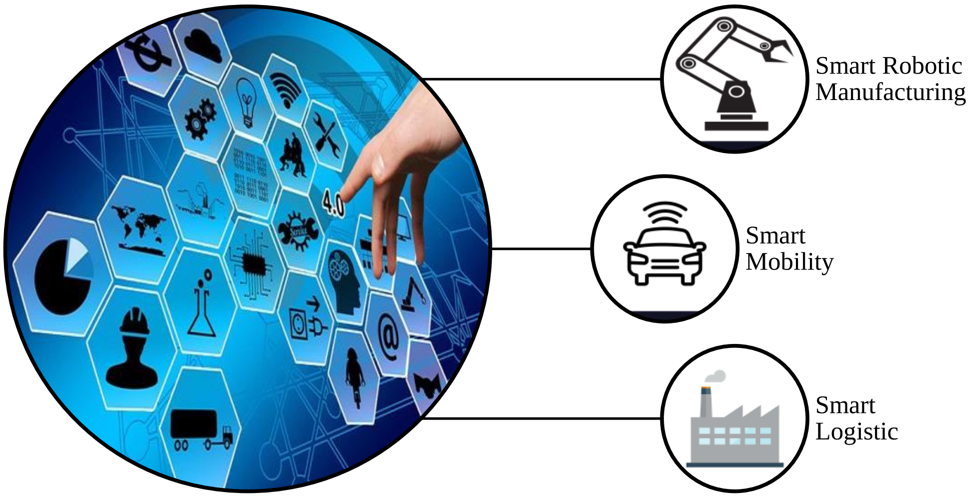


Figure 15. Smart industry features.

5. IoT Communication Protocols

IoT protocols are a vital aspect of the IoT infrastructure stack; hardware is worthless without them because the IoT protocols allow it to communicate data in a standardized and functional manner. Useful knowledge may be derived from these exchanged pieces of data for the end consumer, and thus the whole project is commercially competitive. The classification of IoT protocols is shown in Figure 16. Moreover, some of the most important IoT protocols are listed in Table 3.

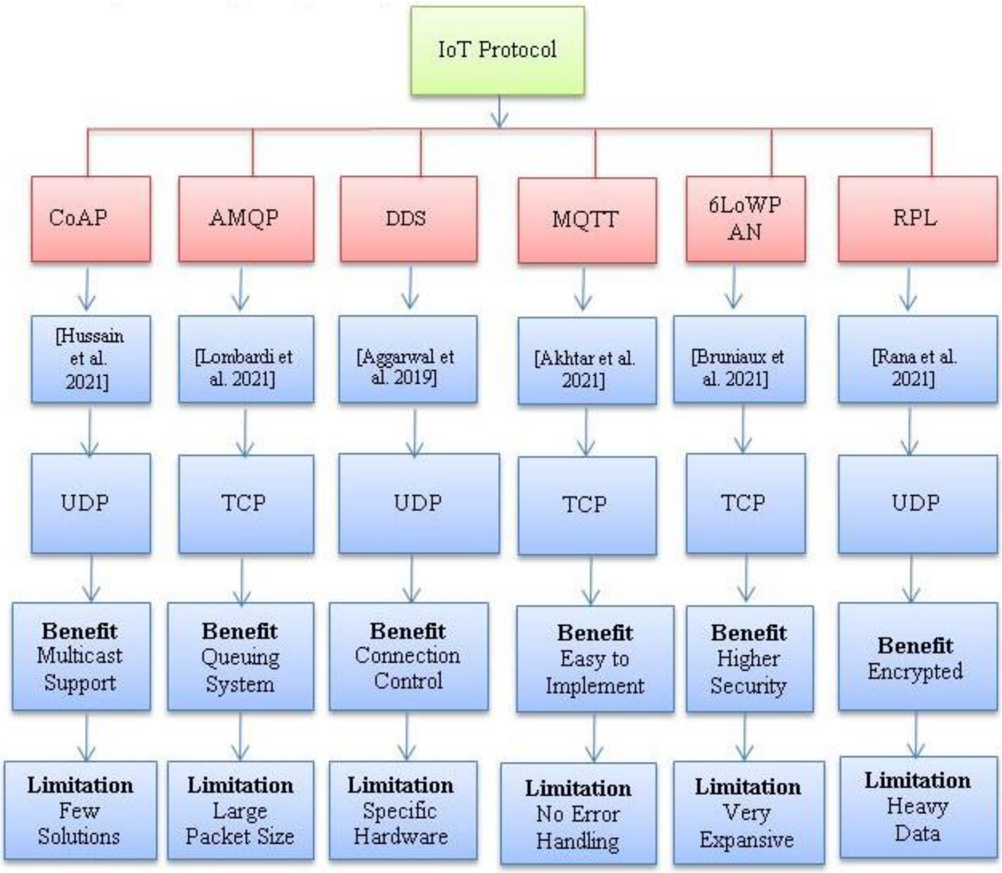


Figure 16. Classification of IoT protocols [82–88].

Table 3. IoT protocols.

Application Protocol	Standard	Transport Protocol	Security	RESTful Support	QoS Support	Architecture
CoAP [82]	IETF RFC 7252	UDP	DTLS	Yes	Yes	Tree
AMQP [83]	ISO and IEC	TCP	TLS/SSL	No	Yes	Client/server
DDS [84]	OMG (Object Management Group)	UDP	DTLS	No	Yes	Bus
MQTT [85]	OASIS Standard	TCP	TLS/SSL	No	Yes	Tree
6LoWPAN [86]	IETF group	TCP	AES	Yes	Yes	Mesh
RPL [87]	IETF group	UDP	AES	No	Yes	Mesh

5.1. Constrained Application Protocol (CoAP)

CoAP is generally used by restricted smart gadgets, i.e., devices that have a similar grouped community. IoT systems using CoAP are driven by HTTP protocols and use a User Datagram Protocol (UDP) for the implementation of lightweight data. Its restful architecture and binary data format make it a perfect fit for applications related to automation, mobile phones and microcontrollers. It employs inside mobiles and interpersonal organization-based applications, and disposes of equivocalness by utilizing the HTTP get, post, put and erase techniques. Aside from imparting IoT information, CoAP has been created alongside DTLS for the safe trade of messages. It utilizes DTLS for the safe exchange of information in the vehicle layer [82].

5.2. Advanced Message Queuing Protocol (AMQP)

AMQP is a middleware-based application layer protocol which was discovered at JP Morgan Chase, London by John O'Hara. MQP is an object layer view for message-arranged middleware conditions. It is an internationally recognized protocol that uses its message-oriented architecture to transfer data via its three prime components of exchange, message queue, and binding. All of these components work collectively to place the parts of the received message in a queue and store it over a connection facilitated by the binding component [83].

5.3. Data Distribution Service (DDS)

DDS is an expandable, high-performance and real-time M2M interacting IoT standard which is capable of transferring data to cloud platforms and low-footprint devices. Through its two layers, Data-Centric Publish–Subscribe (DCPS) and Data Local Reconstruction Layer (DLRL), a data distribution service delivers information to a platform in an intuitive manner [84].

5.4. Message Queue Telemetry Transport (MQTT)

In 1999, MQTT was discovered by Andy Stanford-Clark of IBM and Arlen Nipper of Arcom. Message Query Telemetry Transport is used extensively for remote monitoring. It is effective in obtaining data from multiple far-off located electronic devices and sharing it with a centralized platform. The MQTT protocol works due to its three major components, the subscriber, publisher, and broker. While the data is generated and transmitted by its subscriber mechanism, the publisher is capable of providing information-routing options. The broker ensures the security of the data being transmitted [85].

5.5. IPv6 over Low-Power Wireless Personal Area Networks Protocol (6LoWPAN)

As the core hardware of the Internet Protocol (IP) network, it is the 6LowPAN network standard, rather than the IoT protocols such as Bluetooth and ZigBee [86], which specifies embedding protocols and header compression. Because multiple Zigbee-certified devices can be connected, Zigbee is an appropriate protocol for the IoT. As more Zigbee devices are connected, the number of communication pathways connecting them grows, reducing the likelihood of a single-point signal failure. Zigbee is interoperable and standardises network and application layers, allowing devices from various manufacturers to communicate with one another. Furthermore, Zigbee is based on the 2.4 GHz frequency band, which can be used without a licence anywhere in the world. Solution providers can sell the same product wherever they are on earth as a result of this. In addition, Zigbee has a data transfer rate of 250 kbit/s across 16 channels. Zigbee is a mesh network, which is a communication system made up of radio nodes that are connected in a mesh topology. The mesh network is distinguished by its high degree of interconnectedness. Each mesh network device functions as a node, connecting to the signal and passing it on to the next device. Zigbee can support up to 65,000 devices in a network while preserving signal strength and data transmission capabilities. Certain networks like Wi-Fi, 802.15.4, and sub-1 GHz ISM will also include the frequency range, physical layer, and communication. Internet protocol version 6 (IPv6) has been a major aspect of the IoT in recent years.

5.6. Routing Protocol for Low Power and Lossy Networks (RPL)

IoT is now being developed particularly in health care and smart environments, adding a large number of low-power sensors and actuators to enhance the way of life and provide the community with new services. The Internet Engineering Task Force (IETF) has developed and standardized RPLs in 2012 as the Low Power and Loss Network (LLN) routing protocol. RPL soon attracted attention and was incorporated with specific applications to test and enhance its performance [87].

5.7. Wi-Fi Protocol

To set up a Wi-Fi network, a device that can send wireless signals such as a phone, computer, or routers is required. A router is used at home to convert an internet connection from a public network to the private network of a home or business. WiFi connects neighboring devices that are within a specified range to the Internet. Another option to utilize WiFi is to establish a WiFi hotspot, in which phones or laptops broadcast a signal to share a wireless or wired internet connection with other devices [88].

6. Key Challenges of IoT

IoT is a combination of fields including cyber technology, telecommunications, software analytics, and farming, which generally have a strong emphasis on maintaining privacy. To preserve the following principles provided below to avoid IoT hampering, the critical commitment of states, civil society, and the private sector will play a crucial role. The problems raised by IoT cannot be solved by existing government mechanisms and analysis programs, because they are too cumbersome and too vocal. These problems include: (a) global governance and standards; (b) emerging economic structures and digital currencies; (c) ethics, social regulation, security, approval, and data-based life; and (d) technical obstacles guided by the need to conserve resources. The classification of several primary IoT challenges can be seen in Figure 17.

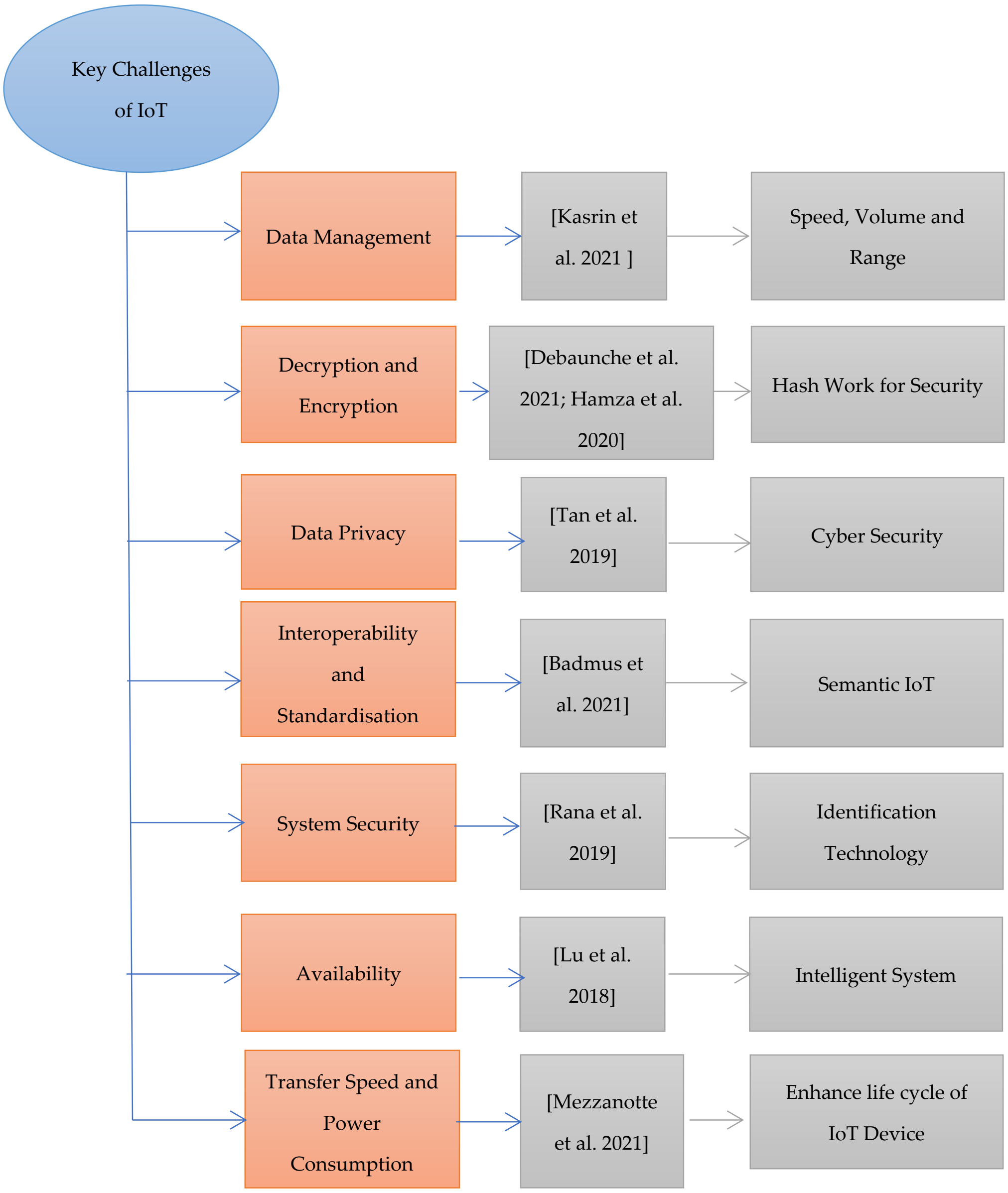


Figure 17. Challenges in IoT [89–98].

6.1. Data Management

Due to billions of IoT devices, data management is the biggest challenge in the present scenario. While there are several other IoT protocols as well as Near Field Communication (NFC), RFID, and Thread, it is important to note that every standard has its distinct specifications and advantages. Studying these specifications is an essential aspect for any company before developing an IoT solution, as protocols are responsible for speed, volume, and range of data transmission. Some examples include bar code obvious affirmation, vision-based article identification, etc. RFID and NFC types of progress are used for disengaging purposes [89].

6.2. Information Decryption and Encryption

Sensor gadgets perform self-governing recognizing or estimations and trade data to the information taking care of the unit over the transmission system with the help of decryption and encryption [90]. An extensive number of gadgets are related to the web. Thus, it is difficult to recognize whether any unapproved gadget partners with a present framework and catch the basic information amid a trade over the web [91]. Thus, classification can be considered the best test for security. Frameworks can consolidate symmetric figures, hash works, and advanced criminological instruments, for instance, code validation and sandboxing [92]. IoT protection focuses on securing the internet-enabled gadgets that link to one another on wireless networks. IoT protection is the security aspect connected to the Internet of Things, which aims to secure IoT devices and networks from cybercrime [93].

6.3. Data Privacy

The IoT uses a distinctive kind of article recognizing confirmation headways, e.g., RFID, 2D-institutionalized labels, etc. As every sort of step-by-step use article will pass on these conspicuous verification marks and add the specific item information, it is vital to take lawful assurance measures and counteract unapproved get-to. IoT ought to work to support straightforward and safe joint customer effort and control. Customers need confidence and the ability to get a handle on the IoT in order to take advantage of its power to secure data privacy. Thus, the major task of the system is to check the privacy of IoT devices [94].

6.4. Interoperability and Standardization

One of the major challenges in the growth of IoT applications is the diversity of technologies and standards. The future of IoT production will be built on the standardization of IoT architecture and communication technologies. These facts suggest that open standards are one of the most important factors in IoT implementation performance. Since they are open to the public, these principles are essential facilitators of creativity. To provide better interoperability for systems using different technologies, they are designed, accepted, and maintained through a collective consensus-based decision-making process [95].

6.5. System Security

The correspondence structure should have the ability to manage data from countless gadgets without any data misfortune in light of framework obstruction, ensure legitimate safety efforts for sending data, and check the security issue. IoT gadgets are poised to be more central in our lives than cell phones, and will push toward the most delicate individual information, for example, government debilitation numbers and banking data, in a way that is exponentially replicated. Even a few security weights on a solitary contraption, for example a telephone, can rapidly swing to 50 or 60 concerns while considering unmistakable IoT gadgets in an interconnected home or business. In light of the vitality that IoT gadgets approach, it is essential to understand their security threats [96].

6.6. Availability

One of the most important problems to address to better manage the complexities of IoT systems is service availability. For any approved object, availability means that IoT applications should be available anywhere and at any time. To support seamless communication and desired availability, the objects that will be linked should be adaptive and intelligent. The network's availability and coverage area must allow for the use of networks to continue regardless of mobility, complex network topology changes, or changes in current technologies. All of this necessitates interoperability, handover, and recovery processes in the event of unattended operations [97].

6.7. Transfer Speed and Power Consumption

There is a need for new calibration and computational techniques as the number of connected objects and data traffic volumes grows dramatically. To support big data, IoT systems need a popular analytic framework that can be provided as a service to IoT apps. Various data mining techniques, such as artificial intelligence (AI), machine learning, and other intelligent decisionmaking algorithms enable computational processes to find patterns in large datasets. These methods can be used to organize raw data as well as extract useful information and knowledge from it, although they are expensive. One of the most pressing concerns is enhancing system capabilities while lowering device costs and power consumption. In addition, one of the main criteria for power and energy efficiency is a low-power communication stack [98].

7. Future Directions

The internet has always been relevant, from industrial machinery to children's toys, and IoT is there to keep the internet safe from abuse. There are many IoT trends coming up for our protection and to keep it healthy. IoT is fundamentally a blend of several new advancements. However, there is no single innovation that can convey the desires of the present for future situations. The classification of future directions in the field of IoT is shown in Figure 18.

7.1. IoT Trends in Transport

In the transportation and logistics industry, the pace of IoT adoption is already high and is continuing to accelerate. By investing in new technology, transport companies are reducing shipping or transportation costs to increase productivity in operations. Predictive diagnostics and vehicle maintenance based on automotive IoT, full transport telematics, and Vehicle-to-Vehicle (V2V) contact are the latest developments in IoT changing the way people and goods are transported [99]. Generalized research insights and implications for transport are:

- In the transportation and logistics industry, the pace of IoT adoption is already high and is continuing to accelerate [100–103].
- The use of data from many IoT devices produces rich videos and images.
- To gain valuable insight into the IoT transportation network, it is required to improve the quality of images and videos.
- For fast-tracking systems, a minimum event detection time is required.
- For real-time tracking of full transport telematics and V2V, minimization of end-to-end delays is required.
- Various methods to protect privacy in terms of such metrics as the position, activity, and description of vehicles must be ensured.

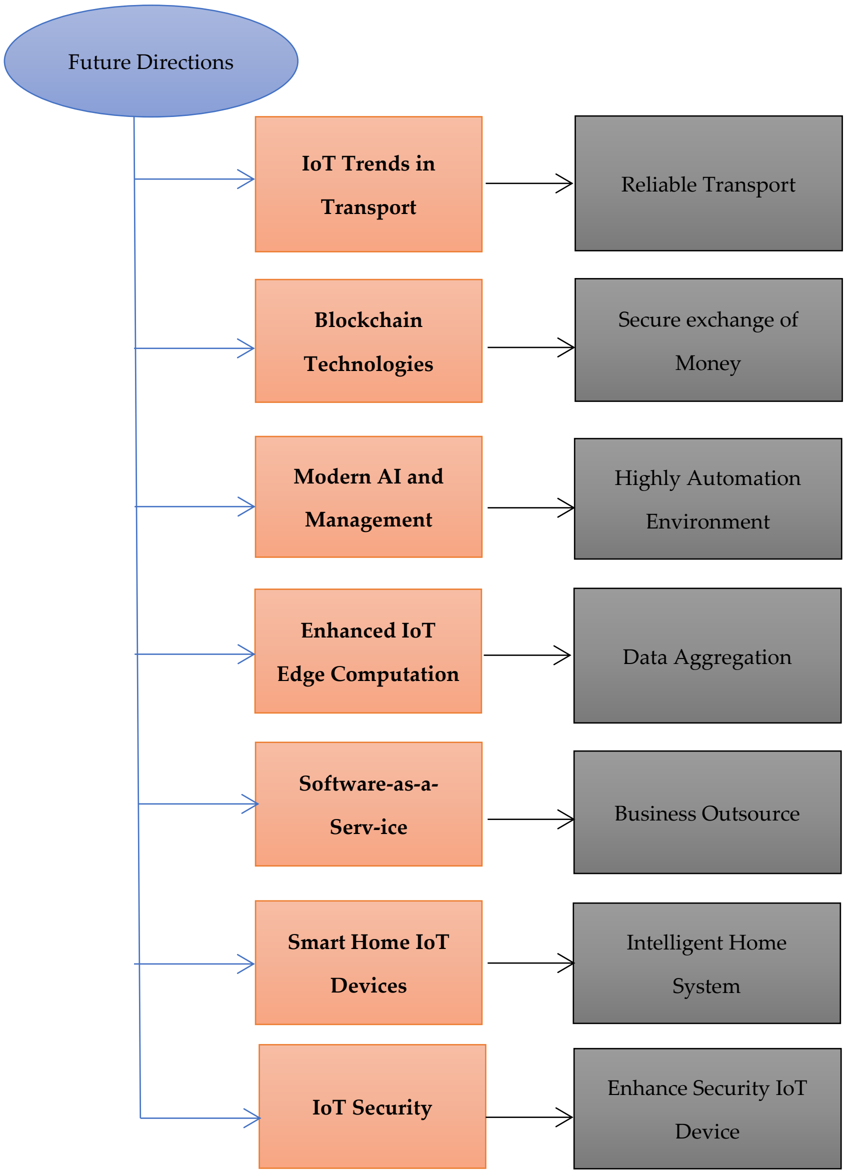


Figure 18. IoT future directions classification.

7.2. Blockchain Technologies

Reliable exchange of money and data between IoT devices becomes possible once blockchain technology provides them with a simple infrastructure to do so. The fragmented nature of IoT is in line with a blockchain's decentralized nature. The latter gives multiple networks and their owners privacy and protection, whilst the digital signatures and private keys that accompany each transaction ensure a secure IoT environment [104]. Generalized research insights and implications for blockchain technologies include:

- As of today, blockchain is one of the main developments in IoT technology.
- For reliable exchange of money and data between IoT devices, blockchain technology should provide efficient infrastructure to do so.
- The owner's privacy and protection should be ensured [105–107].

7.3. Modern Artificial Intelligence and Management

It would be incomplete to list the emerging developments in IoT without considering Artificial Intelligence (AI). In the most complex cases, combinations involving the Internet of Things, blockchain and artificial intelligence arise. The rise in data is one of the biggest causes of change and underlies many of the developments in the IoT market [108]. Generalized research insights and implications for AI technologies are:

- IoT privacy, security, and their link during operations should be taken into account when using IoT for healthcare applications.
- In health IoT systems, powerful analytic methods are required for emergency cases.
- Methods should be given to ensure privacy security such as patient location, name, and records [109–112].

7.4. Enhanced IoT Edge Computation

Edge computing is one of the biggest developments in the IoT industry at present. Connected to IoT devices and applications, the edge nodes and gateways help to access various data center styles. IoT data can also move from the data center to the computer over long distances [113]. Generalized research insights and implications for IoT edge computation include:

- Data in data centres manages all the processes in IoT.
- Focus on the reliability of the network that is used to run the IoT applications [114].

7.5. Software-as-a-Service

Software-as-a-Service (SaaS) has already been deemed a popular subject for conversation for anyone speaking about IoT device developments. SaaS is a type of operation in which a platform houses the target functionality and allows it to open to consumers on the Web [115]. Generalized research insights and implications for SaaS are:

- It lets businesses outsource Information Technology (IT) projects [116].
- Related trends in IoT allow businesses a communications outlet for promotion.

7.6. Smart Home IoT Devices

Even those who first rejected the technologies of smart houses and later embraced them as a blessing can hardly escape the appeal of IoT smart home apps. In the coming years, these devices will be popular and can be expected to dominate other future IoT trends in 2021. Such mobile apps can slowly become increasingly creative and give tremendous assistance to consumers through the use of advanced technologies. Intelligent home appliances not only provide great convenience but also make families more comfortable and happy at home [117]. Generalized research insights and implications for smart home technologies are:

- In the future, IoT devices for smart cities and homes will be popular and will dominate other future IoT trends in 2021.
- Security and privacy are the main concerns when designing and developing a smart city and home IoT devices [118–122].

7.7. IoT Security

With more and more apps linking items to the internet, vast amounts of knowledge can be accessed across various networks. More detail becomes a danger as the network grows. Therefore, it is necessary to maintain secure IoT protection to protect data from manipulation and malicious attacks through the use of IoT. Like all other IoT developments, this will prove to be a significant one in the near future. Throughout the coming years, IoT health will become a significant focus for the easier and better production of smartphone applications focused on IoT. Data are at higher danger in the cloud [123]. Generalized research insights and implications for IoT security are:

- When developing IoT systems, security and privacy issues should be considered.
- Safe systems for information delivery should be developed and applied.
- Compared with other conventional IoT systems, the architecture of the IoT system for the delivery of information should be economical.
- Security and privacy are the main concerns while designing IoT devices [124–127].

8. Importance of Blockchain and Big Data Analytics in IoT

Big Data has been around for a long time, and blockchain technology is currently riding the crest of a wave of popularity. The addition of blockchain to the Big Data analytics process adds another data layer. The ledger's data can be related to energy trade, real estate, and a variety of other fields. This fact has resulted in a slew of Big Data analytics enhancements [128]. For example, fraud protection is possible thanks to blockchain technology, which allows financial institutions to monitor each transaction in real time. As a result, rather than reviewing the records of previous frauds, banks are now able to identify dangerous or fraudulent transactions on the fly, preventing fraud entirely. The importance of these emerging technologies in IoT is discussed below.

8.1. Big Data Analytics in IoT

Over the past several years, the IoT has become an integral part of our daily lives. A large number of sensors or intelligent gadgets have been combined to link humans to the real environment, generating vast amounts of sensing data in the process. IoT device data is gathered, distributed, and transferred among individuals, businesses, and society. The quantity of data created by enterprises or people has increased considerably as a result of the growth of IoT. Despite the great benefit of the huge amount of data created in the IoT environment, researching and utilising this data's amazing worth will increase the danger of privacy violation [129]. The acquisition, storage, and reuse of data for financial gain presents a severe danger to privacy. As a result, researchers have the difficult task of ensuring data utility while maintaining privacy. In order to preserve data privacy, a variety of strategies have been created. These data privacy approaches may be classified into three categories depending on the stages of the big data life cycle [130].

IoT systems are made up of a large number of devices and sensors that interact with one another. The number of these sensors and devices is continuously expanding due to the significant growth and extension of the IoT network [131]. These gadgets connect and send large amounts of data via the internet. This data is massive and updated every second, earning it the moniker "big data". With the continued growth of IoT-based networks, complicated issues such as data management and collection, storage and processing, and analytics can arise [132]. An IoT big data framework for smart buildings may help with a variety of challenges in smart buildings, including monitoring oxygen levels, measuring smoke and hazardous gases, and determining brightness. Such a framework is capable of collecting data from building sensors and doing data analytics for decision-making [133]. Furthermore, an IoT-based cyber-physical system equipped with information analysis and knowledge acquisition methodologies might boost industrial productivity. In smart cities, traffic congestion is a major concern. IoT devices and sensors embedded in traffic signals can collect real-time traffic information, which can then be processed in an IoT-based traffic management system [134].

In healthcare analysis, IoT sensors attached to patients create a large amount of data regarding their health status every second. This vast volume of data must be consolidated into a single database and analyzed in real-time to make rapid, accurate decisions, and big data technology is the best tool for the task. In conjunction with big data analytics, IoT can also aid in the transformation of conventional industrial techniques into new ones [135]. Furthermore, cloud computing and analytics may aid in the development and conservation of energy while lowering costs and increasing customer satisfaction. IoT devices create a large volume of streaming data that must be efficiently stored and analyzed to make real-time decisions. Deep learning is particularly adept at dealing with enormous amounts of data, and can produce very accurate results. As a result, combining IoT, Big Data Analytics, and Deep Learning is critical for the development of a high-tech civilization [136].

8.2. Blockchain Analytics in IoT

We are now surrounded by a plethora of IoT devices and sensors. These gadgets are intended to make life easier and more pleasant. Blockchain technology, particularly its widespread implementation, is quickly becoming a household name. There are still obstacles to overcome when it comes to integrating blockchains into corporate networks. The use of blockchain technology can improve network security and efficiency [137–139]. The blockchain's main property, immutability, makes it resistant to illegal changes. Because a blockchain stores the whole history of device configuration modifications, recovering after an event is simple. A blockchain, also known as a distributed shared ledger, is a cryptographically secure store of records. Devices that download a configuration file from a centralized server must have faith in that authority, and if that trust is broken, the device becomes susceptible. There is no need for a central authority with a blockchain. Peer-to-peer exchanges allow devices to trade assets directly with one another [140–143].

The blockchain has a few essential characteristics that set it apart from other databases. For starters, it is automatically dispersed. It is futile to try to build a blockchain network with only one node. Next, blockchain records are immutable, which means they cannot be deleted or modified. This would invalidate their validity. Only by adding a fully new record may records be updated. In this manner, a safe history of all modifications may be retained. Smart contracts (chaincode) are used on the blockchain to ensure that pre-set business rules are followed correctly [144]. A smart contract is a computer program or agreement that is run by nodes on a blockchain for automation. Devices should be connected wirelessly, opening up new opportunities for system interactions as well as additional choices for device control and tracking and the introduction of sophisticated service capabilities [145]. When compared to network devices in business contexts, IoT devices are constrained by design, with limitations on available resources and performance. When creating a management and monitoring system for IoT devices, this must be taken into account. Different settings and levels of monitoring are used by the heterogeneity of IoT devices for diverse goals. Because business network settings include a similar variety of devices, current network monitoring and management tools may be adapted for IoT implementation [146–150].

9. Conclusions

Recent advances in IoT have drawn the attention of researchers and developers all over the world. IoT developers and researchers are collaborating to bring these technologies to a wider audience and to benefit society as much as possible. However, improvements are only possible if we take into account the various issues and flaws in current technical approaches. To provide intelligent services, IoT must allow seamless communication anywhere, for anyone and anything. This includes detecting, sensing, networking, encoding, and visualization capabilities. This concept has opened up a slew of new possibilities for large-scale service and product development, resulting in many new ideas and business opportunities. The technological standards required for IoT implementation is explored in this review paper. Furthermore, basic communication entities and networks that underpin IoT are examined to anticipate challenges with IoT implementation. We have discussed several issues and challenges that IoT developers must consider when developing a better model, and most importantly, IoT application areas in which IoT developers and researchers are currently involved are presented. This research also contains a detailed review of protocols used for various applications and the security issues involved in implementing the IoT. Future research directions, implementation challenges, and open issues are also reviewed for real-time scenarios.

Author Contributions: Conceptualization, A.K. and S.S.; methodology, A.S., A.A. and B.-J.C.; validation, A.O.-M. and N.G.; formal analysis, A.K. and A.O.-M.; investigation, A.S. and B.-J.C.; resources, A.A. and J.M.-B.; data curation, S.S., A.O.-M.; writing—original draft preparation, A.K., J.M.-B. and N.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by Researchers Supporting Project number (RSP-2021/309), King Saud University, Riyadh, Saudi Arabia, and the research was also supported by the National Research Foundation (NRF) Korea (2019R1C1C1007277) funded by the Ministry of Science and ICT (MSIT)

Korea and by the Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0017123, The Competency Development Program for Industry Specialist).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

List of Abbreviations	**Definition**
A-SEP	Advance Stable Election Protocol
AMQP	Advanced Message Queuing Protocol
CoAP	Constrained Application Protocol
CPS	Cyber-Physical System
DCPS	Data-Centric Publish-Subscribe
DDS	Data Distribution Service
DoS	Denial of Service
DLRL	Data Local Reconstruction Layer
DTLS	Datagram Transport Layer Security
GIS	Geographic Information System
HetNet	Heterogeneous Networks
ICT	Information and Communication Technology
IPv6	Internet Protocol version 6
IETF	Internet Engineering Task Force
LSH	Locality-Sensitive Hashing
LEACH	Low-Energy Adaptive Clustering Hierarchy
LLN	Low-Power and Lossy Network
MAC	Medium Access Control
MEN	Mobile Edge Nodes
MQTT	Message Queue Telemetry Transport
OT	Operative Technology
PIR	Proximity infra-red
RPL	Routing Protocol for Low Power and Lossy Network
RFID	Radio Frequency Identification
SEP	Stable Election Protocol
SSN	System Security Networking
V2V	Vehicle-To-Vehicle

References

1. Hajjaji, Y.; Boulila, W.; Farah, I.R.; Romdhani, I.; Hussain, A. Big data and IoT-based applications in smart environments: A systematic review. *Comput. Sci. Rev.* **2021**, *39*, 100318. [CrossRef]
2. Chegini, H.; Naha, R.K.; Mahanti, A.; Thulasiraman, P. Process Automation in an IoT–Fog–Cloud Ecosystem: A Survey and Taxonomy. *IoT* **2021**, *2*, 92–118. [CrossRef]
3. Zhang, Y.; Sun, Y.; Jin, R.; Lin, K.; Liu, W. High-performance isolation computing technology for smart IoT healthcare in cloud environments. *IEEE Internet Things J.* **2021**, *8*, 16872–16879. [CrossRef]
4. Jacob, T.P.; Pravin, A.; Ramachandran, M.; Al-Turjman, F. Differential spectrum access for next generation data traffic in massive-IoT. *Microprocess. Microsyst.* **2021**, *82*, 103951. [CrossRef]
5. Kuwahara, Y.; Aihara, N.; Yamazaki, S.; Ohuchi, K.; Mizuno, H. Energy-Efficiency Comparison of Ad-hoc Routings in a Shadowing Environment for Smart IoT. In Proceedings of the 2021 International Conference on Information Netw. (ICOIN), Jeju Island, Korea, 13–16 January 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 801–804.
6. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT* **2021**, *2*, 163–188. [CrossRef]
7. Ojanperä, T.; Mäkelä, J.; Majanen, M.; Mämmelä, O.; Martikainen, O.; Väisänen, J. Evaluation of LiDAR data processing at the mobile network edge for connected vehicles. *EURASIP J. Wirel. Commun. Netw.* **2021**, *1*, 1–23. [CrossRef]

8. Rana, A.K.; Sharma, S. Industry 4.0 Manufacturing Based on IoT, Cloud Computing, and Big Data: Manufacturing Purpose Scenario. In *Advances in Communication and Computational Technology*; Singh Hura, G., Singh, A.K., Hoe, L.S., Eds.; Springer: New York, NY, USA; Singapore, 2021; pp. 1109–1119.
9. Oktian, Y.E.; Witanto, E.N.; Lee, S.G. A Conceptual Architecture in Decentralizing Computing, Storage, and Networking Aspect of IoT Infrastructure. *IoT* **2021**, *2*, 205–221. [CrossRef]
10. Almezhghwi, K.; Serte, S.; Al-Turjman, F. Convolutional neural networks for the classification of chest X-rays in the IoT era. *Multimed. Tools Appl.* **2021**, *12*, 1–15. [CrossRef]
11. Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* **2020**, *61*, 102360. [CrossRef]
12. Bhushan, B.; Sahoo, C.; Sinha, P.; Khamparia, A. Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. *Wirel. Netw.* **2021**, *27*, 55–90. [CrossRef]
13. Inam, H.; Al-Turjman, F. Intelligent free energy usage through radiant energy space phenomenon: An IoT-powered prototype for modified Bedini generator. *Microprocess. Microsyst.* **2021**, *21*, 104319. [CrossRef]
14. Jamil, H.; Umer, T.; Ceken, C.; Al-Turjman, F. Decision Based Model for Real-Time IoT Analysis Using Big Data and Machine Learning. *Wirel. Pers. Commun.* **2021**, *121*, 2747–2959. [CrossRef]
15. Xu, L.; Wu, H.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
16. Alhamoud, A.; Ruettiger, F.; Reinhardt, A.; Englert, F.; Burgstahler, D. Smartenergy. kom: An intelligent system for energy saving in smart home. In Proceedings of the 39th Annual IEEE Conference on Local Computer Networks Workshops, Edmonton, AB, Canada, 8–11 September 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 685–692.
17. Akkaya, K.; Guvenc, I.; Aygun, R.; Pala, N.; Kadri, A. IoT-based occupancy monitoring techniques for energy-efficient smart buildings. In Proceedings of the 2015 IEEE Wireless Communications and Network Conference Workshops (WCNCW), New Orleans, LA, USA, 9–12 March 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 58–63.
18. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *141*, 22–32. [CrossRef]
19. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, S. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
20. Abdur, A.; Qureshi, M.; Gill, S.; Ullah, S. Security issues in the Internet of Things (IoT): A comprehensive study. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 383. [CrossRef]
21. Raja, A.; Naveedha, R.; Niranjanadevi, G.; Roobini, V. An internet of things (IoT) based security alert system using raspberry pi. *Asia Pac. Int. J. Eng. Sci.* **2016**, *2*, 37–41.
22. Tahir, H.; Kanwer, A.; Junaid, M. Internet of Things (IoT): An overview of applications and security issues regarding implementation. *Int. J. Multidiscip. Sci. Eng.* **2016**, *7*, 14–22.
23. Wang, Y.; Zhang, M.; Shu, W. An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2018**, *1*, 45. [CrossRef]
24. Zhu, X.; Ding, B.; Li, W.; Gu, L.; Yang, Y. On development of security monitoring system via wireless sensing network. *EURASIP J. Wirel. Commun. Netw.* **2018**, *1*, 221. [CrossRef]
25. Suchitra, C.; Vandana, C.P. Internet of things and security issues. *Int. J. Comput. Sci. Mob. Comput.* **2016**, *5*, 133–139.
26. Zhang, W.; Kumar, M.; Yu, J.; Yang, J. Medical long-distance monitoring system based on internet of things. *EURASIP J. Wirel. Commun. Netw.* **2018**, *1*, 1–8. [CrossRef]
27. Wang, D.; Xu, L.; Wang, F.; Xu, Q. An anonymous batch handover authentication protocol for big flow wireless mesh networks. *EURASIP J. Wirel. Commun. Netw.* **2018**, *1*, 1–8. [CrossRef]
28. Afanasyev, I.; Mazzara, M.; Chakraborty, S.; Zhuchkov, N.; Maksatbek, A.; Yesildirek, A.; Kassab, M.; Distefano, S. Towards the internet of robotic things: Analysis, architecture, components and challenges. In Proceedings of the 2019 12th International Conference on Developments in eSystems Engineering (DeSe), Kazan, Russia, 7–10 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 3–8.
29. Dharshini, S.; Subashini, M.M. An overview on wireless body area networks. In Proceedings of the 2017 Innovations in Power and Advanced Computing Technologies (i-PACT 2017), Vellore, India, 21–22 April 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–10.
30. Alezabi, K.A.; Hashim, F.; Hashim, S.J.; Ali, B.M.; Jamalipour, A. Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks. *EURASIP J. Wirel. Commun. Netw.* **2020**, *77*, 1–34. [CrossRef]
31. Weber, R.H. Internet of things-new security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
32. Toor, A.; ul Islam, S.; Ahmed, G.; Jabbar, S.; Khalid, S.; Sharif, A.M. Energy efficient edge-of-things. *EURASIP J. Wirel. Commun. Netw.* **2020**, *1*, 82. [CrossRef]
33. Liu, J.; Xiao, Y.; Philip-Chen, C.L. Hybrid content-based routing using network and application layer filtering. In Proceedings of the IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 27–30 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 221–231.
34. Huang, S.; Zhu, L.; Liu, S. Based on virtual beamforming cooperative jamming with Stackelberg game for physical layer security in the heterogeneous wireless network. *EURASIP J. Wirel. Commun. Netw.* **2018**, *1*, 69. [CrossRef]

35. Li, Y.; Alqahtani, A.; Solaiman, E.; Perera, C.; Jayaraman, P.P.; Buyya, R.; Morgan, G.; Ranjan, R. IoT-CANE: A unified knowledge management system for data-centric Internet of Things application systems. *J. Parallel Distrib. Comput.* **2019**, *131*, 161–172. [CrossRef]
36. Pierleoni, P.; Conti, M.; Belli, A.; Palma, L.; Incipini, L.; Sabbatini, L.; Valenti, S.; Mercuri, M.; Concetti, R. Iot solution based on MQTT protocol for real-time building monitoring. In Proceedings of the 2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT), Ancona, Italy, 19–21 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 57–62.
37. Luk, M.; Mezzour, G.; Perrig, A.; Gligor, V. MiniSec: Secure sensor network communication architecture. In Proceedings of the 6th International Conference on Information Processing in Sensor Networks, Cambridge, MA, USA, 25–27 April 2007; Association for Computing Machinery: New York, NY, USA, 2007.
38. Li, Q.; Ning, H.; Zhu, T.; Cui, S.; Chen, L. A hybrid approach to inferring the Internet of Things for complex activity recognition. *EURASIP J. Wirel. Commun. Netw.* **2019**, *1*, 251. [CrossRef]
39. Xiang, X.; Liu, W.; Wang, T.; Xie, M.; Li, X.; Song, H.; Liu, A.; Zhang, G. Delay and energy-efficient data collection scheme-based matrix filling theory for dynamic traffic IoT. *EURASIP J. Wirel. Commun. Netw.* **2019**, *1*, 168. [CrossRef]
40. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]
41. Novosel, L.; Šišul, G. Performance evaluation of chaotic spreading sequences on software-defined radio. *EURASIP J. Wirel. Commun. Netw.* **2017**, *1*, 80. [CrossRef]
42. Wu, M.; Wu, Y.; Liu, X.; Ma, M.; Liu, A.; Zhao, M. Learning-based synchronous approach from forwarding nodes to reduce the delay for Industrial Internet of Things. *EURASIP J. Wirel. Commun. Netw.* **2018**, *1*, 10. [CrossRef]
43. Stergiou, C.L.; Psannis, K.E.; Gupta, B.B. IoT-based Big Data secure management in the Fog over a 6G Wireless Network. *IEEE Internet Things J.* **2020**, *8*, 5164–5171. [CrossRef]
44. Temglit, N.; Chibani, A.; Djouani, K.; Sacer, M.A. A distributed agent-based approach for optimal QoS selection in web of object choreography. *IEEE Syst. J.* **2018**, *12*, 1655–1666. [CrossRef]
45. Wan, J.; Al-awlaqi, M.A.; Li, M.; O'Grady, M.; Gu, X.; Wang, J.; Cao, N. Wearable IoT enabled real-time health monitoring system. *EURASIP J. Wirel. Commun. Netw.* **2018**, *1*, 1–10. [CrossRef]
46. Ali, A.M.; Al Ghamdi, M.A.; Iqbal, M.M.; Khalid, S.; Aldabbas, H.; Saeed, S. Next-generation UWB antennas gadgets for human health care using SAR. *EURASIP J. Wirel. Commun. Netw.* **2021**, *1*, 33. [CrossRef]
47. Liu, Q.; Sun, S.; Yuan, X. Ambient backscatter communication-based smart 5G IoT network. *EURASIP J. Wirel. Commun. Netw.* **2021**, *1*, 34. [CrossRef]
48. Majeed, S.; Sohail, A.; Qureshi, K.N.; Kumar, A.; Iqbal, S.; Lloret, J. Unmanned aerial vehicles optimal airtime estimation for energy aware deployment in IoT-enabled fifth generation cellular networks. *EURASIP J. Wirel. Commun. Netw.* **2020**, *1*, 254. [CrossRef]
49. Jebarani, M.E.; Kumaraguru, S. Secured Human Health Monitoring Using Wireless Medical Sensor Networks Review. *Eur. J. Mol. Clin. Med.* **2020**, *7*, 1913–1924.
50. Raji, M.F.; Li, J.; Haq, A.U.; Ejianya, V.; Khan, J.; Khan, A.; Khalil, M.; Ali, A.; Shahid, M.; Ahamad, B.; et al. A New Approach for Enhancing the Services of the 5G Mobile Network and IOT-Related Communication Devices Using Wavelet-OFDM and Its Applications in Healthcare. *Sci. Program.* **2020**, *10*, 2020. [CrossRef]
51. Palattella, M.R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 510–527. [CrossRef]
52. Mothukuri, V.; Khare, P.; Parizi, R.M.; Pouriyeh, S.; Dehghantanha, A.; Srivastava, G. Federated Learning-based Anomaly Detection for IoT Security Attacks. *IEEE Internet Things J.* **2021**. [CrossRef]
53. Behera, T.M.; Mohapatra, S.K.; Samal, U.C.; Khan, M.S.; Daneshmand, M.; Gandomi, A.H. Residual energy-based cluster-head selection in WSNs for IoT application. *IEEE Internet Things J.* **2019**, *6*, 5132–5139. [CrossRef]
54. Farman, H. Multi Criterion based zone head selection in Internet of Things based on wireless sensor networks, future generation. *Future Gener. Comput. Syst.* **2018**, *87*, 364–371. [CrossRef]
55. Behera, M.; Samal, U.; Mohapatra, K. Energy efficient modified LEACH protocol for IoT applications. *IET Wirel. Sens. Syst.* **2018**, *8*, 223–228. [CrossRef]
56. Butler, D. Computing: Everything, everywhere. *Nature* **2020**, *440*, 402–405. [CrossRef] [PubMed]
57. Hu, L.; Liu, A.; Xie, M.; Wang, T. UAVs joint vehicles as data mules for fast codes dissemination for edge network in smart city. *Peer-Peer Netw. Appl.* **2019**, *12*, 1550–1574. [CrossRef]
58. Alzahrani, B.A.; Irshad, A.; Albeshri, A.; Alsubhi, K. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. *Wirel. Pers. Commun.* **2021**, *117*, 47–69. [CrossRef]
59. Wang, T.; Qiu, L.; Xu, G.; Sangaiah, A. Energy-efficient and trustworthy data collection protocol based on mobile fog computing in Internet of Things. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3531–3539. [CrossRef]
60. Qi, L.; Wang, R.; Hu, C.; Li, S.; He, Q.; Xu, X. Time-aware distributed service recommendation with privacy-preservation. *Inf. Sci.* **2019**, *480*, 354–364. [CrossRef]
61. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]
62. Marche, C.; Nitti, M. A Binary Trust Game for the Internet of Things. *IoT* **2021**, *1*, 50–70. [CrossRef]

63. Wang, T.; Luo, H.; Zheng, X.; Xie, M. Crowd sourcing mechanism for trust evaluation in CPCS based on intelligent mobile edge computing. *ACM Transection Intell. Syst. Technol.* **2019**, *10*, 1–19.
64. Khraisat, A.; Alazab, A. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2021**, *4*, 18. [CrossRef]
65. Haris, M.; Al-Maadeed, S. Integrating Blockchain Technology in 5G enabled IoT: A Review. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 367–371.
66. Srivastav, H.; Dwivedi, R. Energy Efficiency in Sensor Based IoT using Mobile Agents: A Review. In Proceedings of the 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Uttar Pradesh, India, 28–29 February 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 314–319.
67. Fu, X.; Ding, T.; Peng, R.; Liu, C.; Cheriet, M. Joint UAV channel modeling and power control for 5G IoT networks. *EURASIP J. Wirel. Commun. Netw.* **2021**, *1*, 106. [CrossRef]
68. Yi, H.; Lin, W.; Huang, X.; Cai, X.; Chi, R.; Nie, Z. Energy Trading IoT System Based on Blockchain. *Swarm Evol. Comput.* **2021**, *37*, 100891. [CrossRef]
69. Gulzar, M.; Abbas, G.; Waqas, M. Climate Smart Agriculture: A Survey and Taxonomy. In Proceedings of the 2020 International Conference on Emerging Trends in Smart Technologies (ICETST), Karachi, Pakistan, 26–27 March 2020; Curran Associates, Inc.: Red Hook, NY, USA, 2020; pp. 1–6.
70. Answer, M.; Ashfaque, A. Security of IoT Using Block chain: A Review. In Proceedings of the 2020 International Conference on Information Science and Communication Technology (ICISCT), Karachi, Pakistan, 8–9 February 2020; Curran Associates, Inc.: Red Hook, NY, USA, 2020; pp. 1–5.
71. Mughal, D.M.; Shah, S.T.; Chung, M.Y. An Efficient Spectrum Utilization Scheme for Energy-Constrained IoT Devices in Cellular Networks. *IEEE Internet Things J.* **2021**, *8*, 13414–13424. [CrossRef]
72. José, V.; Sobral, V. Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications. *Sensors* **2019**, *19*, 2144.
73. Jangid, A.; Dubey, P.; Chandavarkar, R. Security issues and challenges in Healthcare Automated Devices. In Proceedings of the 12th International Conference on Communication Systems and Networks (COMSNETS 2020), Bengaluru, India, 7–11 January 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 19–23.
74. Mocnej, J.; Pekar, A.; Seah, W.K.; Papcun, P.; Kajati, E.; Cupkova, D.; Koziorek, J.; Zolotova, I. Quality-enabled decentralized IoT architecture with efficient resources utilization. *Robot. Comput. Integr. Manuf.* **2021**, *67*, 102001. [CrossRef]
75. Sarrab, M.; Alshohoumi, F. Assisted-Fog-Based Framework for IoT-Based Healthcare Data Preservation. *Int. J. Cloud Appl. Comput.* **2021**, *11*, 1–6. [CrossRef]
76. Goyal, S.; Sharma, N.; Bhushan, B.; Shankar, A.; Sagayam, M. Iot enabled technology in secured healthcare: Applications, challenges and future directions. In *Cognitive Internet of Medical Things for Smart Healthcare 2021*; Hassanien, E., Khamparia, A., Gupta, D., Shankar, K., Slowik, A., Eds.; Springer: Cham, Switzerland, 2021; pp. 25–48.
77. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-based authentication and authorization for smart city applications. *Inf. Process. Manag.* **2021**, *58*, 102468. [CrossRef]
78. Maddikunta, P.K.; Hakak, S.; Alazab, M.; Bhattacharya, S.; Gadekallu, T.R.; Khan, W.Z.; Pham, Q.V. Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges. *IEEE Sens. J.* **2021**, *13*, 78–98. [CrossRef]
79. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
80. Labus, A.; Radenković, B.; Rodić, B.; Barać, D.; Malešević, A. Enhancing smart healthcare in dentistry: An approach to managing patients' stress. *Inform. Health Soc. Care* **2021**, *1*, 306–319. [CrossRef] [PubMed]
81. Zahra, S.R.; Chishti, M.A. Smart Cities Pilot Projects: An IoT Perspective. In *Smart Cities: A Data Analytics Perspective*; Ayoub Khan, M., Algarni, F., Tabrez Quasim, M., Eds.; Springer: Cham, Switzerland, 2021; pp. 231–255.
82. Hussain, A.; Ali, T.; Althobiani, F.; Draz, U.; Irfan, M.; Yasin, S.; Shafiq, S.; Safdar, Z.; Glowacz, A.; Nowakowski, G.; et al. Security Framework for IoT Based Real-Time Health Applications. *Electronics* **2021**, *10*, 719. [CrossRef]
83. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information* **2021**, *12*, 87. [CrossRef]
84. Agarwal, T.; Niknejad, P.; Barzegaran, M.R.; Vanfretti, L. Multi-level Time-Sensitive Network (TSN) using the Data Distribution Services (DDS) for Synchronized Three-Phase Measurement Data Transfer. *IEEE Access* **2019**, *7*, 131407–131417. [CrossRef]
85. Akhtar, S.; Zahoor, E. Formal Specification and Verification of MQTT Protocol in PlusCal-2. *Wirel. Pers. Commun.* **2021**, *22*, 1589–1606. [CrossRef]
86. Bruniaux, A.; Koutsiamanis, R.A.; Papadopoulos, G.Z.; Montavont, N. Defragmenting the 6LoWPAN Fragmentation Landscape: A Performance Evaluation. *Sensors* **2021**, *5*, 1711. [CrossRef] [PubMed]
87. Rana, A.K.; Sharma, S. Contiki Cooja Security Solution (CCSS) with IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) in Internet of Things Applications. In *Mobile Radio Communications and 5G Networks*; Springer: Singapore, 2021; pp. 251–259.
88. Pancaroglu, D.; Sen, S. Load balancing for RPL-based Internet of Things: A review. *Ad Hoc Netw.* **2021**, *18*, 102491. [CrossRef]
89. Kasrin, N.; Benabbas, A.; Elmamooz, G.; Nicklas, D.; Steuer, S.; Sünkel, M. Data-sharing markets for integrating IoT data processing functionalities. *CCF Trans. Pervasive Comput. Interact.* **2021**, *13*, 76–93. [CrossRef]

90. Debauche, O.; Trani, J.P.; Mahmoudi, S.; Manneback, P.; Bindelle, J.; Mahmoudi, S.; Lebeau, F. Data Management and Internet of Things: A Methodological Review in Smart Farming. *Internet Things* **2021**, *15*, 100378. [CrossRef]
91. Chandu, Y.; Kumar, K.R.; Prabhukhanolkar, N.V.; Anish, A.N.; Rawal, S. Design and implementation of hybrid encryption for security of IOT data. In Proceedings of the 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bengaluru, India, 17–19 August 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1228–1231.
92. Kumar, A.; Sharma, S.; Goyal, N.; Gupta, S.K.; Kumari, S.; Kumar, S. Energy-efficient fog computing in Internet of Things based on Routing Protocol for Low-Power and Lossy Network with Contiki. *Int. J. Commun. Syst.* **2021**, *87*, e5049. [CrossRef]
93. Hamza, R.; Yan, Z.; Muhammad, K.; Bellavista, P.; Titouna, F. A privacy-preserving cryptosystem for IoT E-healthcare. *Inf. Sci.* **2020**, *527*, 493–510. [CrossRef]
94. Tan, X.; Su, S.; Huang, Z.; Guo, X.; Zuo, Z.; Sun, X.; Li, L. Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm. *Sensors* **2019**, *19*, 203. [CrossRef]
95. Badmus, I.; Laghrissi, A.; Matinmikko-Blue, M.; Pouttu, A. End-to-end network slice architecture and distribution across 5G micro-operator leveraging multi-domain and multi-tenancy. *EURASIP J. Wirel. Commun. Netw.* **2021**, *1*, 1–23. [CrossRef]
96. Rana, A.K.; Krishna, R.; Dhwan, S.; Sharma, S.; Gupta, R. Review on artificial intelligence with internet of things-problems, challenges and opportunities. In Proceedings of the 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), Greater Noida, India, 18–19 October 2019; pp. 383–387.
97. Lu, D.; Ding, C.; Xu, J.; Wang, S. Hierarchical discriminant analysis. *Sensors* **2018**, *18*, 279. [CrossRef]
98. Mezzanotte, P.; Palazzi, V.; Alimenti, F.; Roselli, L. Innovative rfid sensors for internet of things applications. *IEEE J. Microw.* **2021**, *1*, 55–65. [CrossRef]
99. Culman, C.; Aminikhanghahi, J.; Cook, D. Easing power consumption of wearable activity monitoring with change point detection. *Sensors* **2020**, *20*, 310. [CrossRef]
100. Centobelli, P.; Cerchione, R.; Esposito, E. Environmental sustainability in the service industry of transportation and logistics service providers: Systematic literature review and research directions. *Transp. Res. Part D Transp. Environ.* **2017**, *53*, 454–470. [CrossRef]
101. Mo, X.; Qian, Q.; Guo, Q.; Cheng, Q. Spatial distribution features of the transportation-oriented logistics enterprises in Guangzhou. *Trop. Geogr.* **2010**, *30*, 521–527.
102. Rey, A.; Panetti, E.; Maglio, R.; Ferretti, M. Determinants in adopting the Internet of Things in the transport and logistics industry. *J. Bus. Res.* **2021**, *131*, 584–590. [CrossRef]
103. Olszewski, R.; Pałka, P.; Turek, A. Solving "Smart City" Transport Problems by Designing Carpooling Gamification Schemes with Multi-Agent Systems: The Case of the So-Called "Mordor of Warsaw". *Sensors* **2018**, *18*, 141. [CrossRef]
104. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
105. Niknejad, N.; Ismail, W.; Bahari, M.; Hendradi, R.; Salleh, A.Z. Mapping the research trends on blockchain technology in food and agriculture industry: A bibliometric analysis. *Environ. Technol. Innov.* **2021**, *21*, 101272. [CrossRef]
106. Budak, A.; Çoban, V. Evaluation of the impact of blockchain technology on supply chain using cognitive maps. *Expert Syst. Appl.* **2021**, *184*, 115455. [CrossRef]
107. Tsao, Y.C.; Thanh, V.V.; Wu, Q. Sustainable microgrid design considering blockchain technology for real-time price-based demand response programs. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106418. [CrossRef]
108. Dhawan, S.; Chakraborty, C.; Frnda, J.; Gupta, R.; Rana, A.K.; Pani, S.K. SSII: Secured and high-quality Steganography using intelligent hybrid optimization algorithms for IoT. *IEEE Access* **2021**, *9*, 87563–87578. [CrossRef]
109. Andronie, M.; Lăzăroiu, G.; Iatagan, M.; Uță, C.; Ștefănescu, R.; Cocoșatu, M. Artificial Intelligence-Based Decision-Making Algorithms, Internet of Things Sensing Networks, and Deep Learning-Assisted Smart Process Management in Cyber-Physical Production Systems. *Electronics* **2021**, *10*, 2497. [CrossRef]
110. Gorris, M.; Hoogenboom, S.A.; Wallace, M.B.; van Hooft, J.E. Artificial intelligence for the management of pancreatic diseases. *Dig. Endosc.* **2021**, *33*, 231–241. [CrossRef]
111. Rana, A.K.; Sharma, S. Internet of Things Based Stable Increased-throughput Multi-hop Protocol for Link Efficiency (IoT-SIMPLE) For Health Monitoring Using Wireless Body Area Networks. *Int. J. Sens. Wirel. Commun. Control.* **2021**, *11*, 789–798. [CrossRef]
112. Gregory, R.W.; Henfridsson, O.; Kaganer, E.; Kyriakou, H. The role of artificial intelligence and data network effects for creating user value. *Acad. Manag. Rev.* **2021**, *46*, 534–551. [CrossRef]
113. Vaiyapuri, T.; Parvathy, V.S.; Manikandan, V.; Krishnaraj, N.; Gupta, D.; Shankar, K. A Novel Hybrid Optimization for Cluster-Based Routing Protocol in Information-Centric Wireless Sensor Networks for IoT Based Mobile Edge Computing. *Wirel. Pers. Commun.* **2021**, *3*, 1–24. [CrossRef]
114. Guillén, M.A.; Llanes, A.; Imbernón, B.; Martínez-España, R.; Bueno-Crespo, A.; Cano, J.C.; Cecilia, J.M. Performance evaluation of edge-computing platforms for the prediction of low temperatures in agriculture using deep learning. *J. Supercomput.* **2021**, *77*, 818–840. [CrossRef]
115. Li, S.; Kim, J.G.; Han, D.H.; Lee, K.S. A Survey of Energy-Efficient Communication Protocols with QoS Guarantees in Wireless Multimedia Sensor Networks. *Sensors* **2019**, *19*, 199. [CrossRef]
116. Mesquita, A.A.; Penha, R.; Kniess, C.T.; Travis, T. Use of sustainability indicators in the management of information technology projects. *Rev. Adm. UFSM* **2021**, *14*, 22–43. [CrossRef]

117. Seneviratne, C.; Wijesekara, P.A.D.S.N.; Leung, H. Performance Analysis of Distributed Estimation for Data Fusion Using a Statistical Approach in Smart Grid Noisy Wireless Sensor Networks. *Sensors* **2020**, *20*, 567. [CrossRef] [PubMed]
118. Kumar, P.; Chouhan, L. Design of secure session key using unique addressing and identification scheme for smart home Internet of Things network. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e3993. [CrossRef]
119. Trabelsi, Z. IoT based Smart Home Security Education using a Hands-on Approach. In Proceedings of the 2021 IEEE Global Engineering Education Conference (EDUCON), Online, 21–23 April 2020; pp. 294–301.
120. Srinivas, P.; Das, M.S.; Latha, Y.M. Future Smart Home Appliances Using IoT. In *Innovations in Computer Science and Engineering*; Saini, H.S., Sayal, R., Govardhan, A., Buyya, R., Eds.; Springer: Singapore, 2021; pp. 143–151.
121. Charde, P. Design and Implement Smart Home Appliances Controller Using IOT. In Proceedings of the 3rd International Conference on Information Systems and Management Science (ISMS), Msida, Malta, 15–17 December 2020; Garg, L., Kesswani, N., Vella, J.G., Xuereb, P.A., Fung Lo, M., Diaz, R., Misra, S., Gupta, V., Randhawa, P., Eds.; Springer Nature: Singapore, 2020; Volume 303, p. 105.
122. Kolanur, C.B.; Banakar, R.M.; Rajneesh, G. Design of IoT based Platform Development for Smart Home Appliances Control. In *Journal of Physics: Conference Series*; IOP Publishing: Bristol, UK, 2021; Volume 1969, p. 012052.
123. Popescu, T.M.; Popescu, A.M.; Prostean, G. IoT Security Risk Management Strategy Reference Model (IoTSRM2). *Future Internet* **2021**, *13*, 148. [CrossRef]
124. Kang, M.S. Design of AES-Based Encryption Chip for IoT Security. *J. Inst. Internet Broadcasting Commun.* **2021**, *21*, 1–6.
125. Chen, T.H.; Lee, W.B.; Chen, H.B.; Wang, C.L. Revisited—The Subliminal Channel in Blockchain and Its Application to IoT Security. *Symmetry* **2021**, *13*, 855. [CrossRef]
126. Bhatt, S.; Ragiri, P.R. Security trends in Internet of Things: A survey. *SN Appl. Sci.* **2021**, *3*, 1–14.
127. Yao, X.; Farha, F.; Li, R.; Psychoula, I.; Chen, L.; Ning, H. Security and privacy issues of physical objects in the IoT: Challenges and opportunities. *Digit. Commun. Netw.* **2021**, *7*, 373–384. [CrossRef]
128. Fathi, M.; Haghi Kashani, M.; Jameii, S.M.; Mahdipour, E. Big data analytics in weather forecasting: A systematic review. *Arch. Comput. Methods Eng.* **2021**, *106*, 1–29. [CrossRef]
129. Chang, V. An ethical framework for big data and smart cities. *Technol. Forecast. Soc. Chang.* **2021**, *165*, 120559. [CrossRef]
130. Sheng, J.; Amankwah-Amoah, J.; Khan, Z.; Wang, X. COVID-19 pandemic in the new era of big data analytics: Methodological innovations and future research directions. *Br. J. Manag.* **2021**, *32*, 1164–1183. [CrossRef]
131. Završnik, A. Algorithmic justice: Algorithms and big data in criminal justice settings. *Eur. J. Criminol.* **2021**, *18*, 623–642. [CrossRef]
132. Kaffash, S.; Nguyen, A.T.; Zhu, J. Big data algorithms and applications in intelligent transportation system: A review and bibliometric analysis. *Int. J. Prod. Econ.* **2021**, *231*, 107868. [CrossRef]
133. Barja-Martinez, S.; Aragüés-Peñalba, M.; Munné-Collado, Í.; Lloret-Gallego, P.; Bullich-Massagué, E.; Villafafila-Robles, R. Artificial intelligence techniques for enabling Big Data services in distribution networks: A review. *Renew. Sustain. Energy Rev.* **2021**, *150*, 111459. [CrossRef]
134. Jaung, W.; Carrasco, L.R. A big-data analysis of human-nature relations in newspaper coverage. *Geoforum* **2022**, *128*, 11–20. [CrossRef]
135. Boeing, G. Spatial information and the legibility of urban form: Big data in urban morphology. *Int. J. Inf. Manag.* **2021**, *56*, 102013. [CrossRef]
136. Novak, A.; Bennett, D.; Kliestik, T. Product decision-making information systems, real-time sensor networks, and artificial intelligence-driven big data analytics in sustainable Industry 4.0. *Econ. Manag. Financ. Mark.* **2021**, *16*, 62–72.
137. Sestrem Ochôa, I.; Augusto Silva, L.; De Mello, G.; Garcia, N.M.; de Paz Santana, J.F.; Quietinho Leithardt, V.R. A cost analysis of implementing a blockchain architecture in a smart grid scenario using sidechains. *Sensors* **2020**, *20*, 843. [CrossRef]
138. Adi, E.; Anwar, A.; Baig, Z.; & Zeadally, S. Machine learning and data analytics for the IoT. *Neural Comput. Appl.* **2020**, *32*, 16205–16233. [CrossRef]
139. Sestrem Ochôa, I.; Reis Quietinho Leithardt, V.; Calbusch, L.; De Paz Santana, J.F.; Delcio Parreira, W.; Oriel Seman, L.; Zeferino, C.A. Performance and Security Evaluation on a Blockchain Architecture for License Plate Recognition Systems. *Appl. Sci.* **2021**, *11*, 1255. [CrossRef]
140. Iftekhar, A.; Cui, X. Blockchain-Based Traceability System That Ensures Food Safety Measures to Protect Consumer Safety and COVID-19 Free Supply Chains. *Foods* **2021**, *10*, 1289. [CrossRef] [PubMed]
141. Shinde, R.; Patil, S.; Kotecha, K.; Ruikar, K. Blockchain for securing ai applications and open innovations. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 189. [CrossRef]
142. Chen, X.; Tian, S.; Nguyen, K.; Sekiya, H. Decentralizing private blockchain-iot network with olsr. *Future Internet* **2021**, *13*, 168. [CrossRef]
143. Ajayi, O.J.; Rafferty, J.; Santos, J.; Garcia-Constantino, M.; Cui, Z. BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems. *IoT* **2021**, *2*, 610–632. [CrossRef]
144. Steenmans, K.; Taylor, P.; Steenmans, I. Blockchain Technology for Governance of Plastic Waste Management: Where Are We? *Soc. Sci.* **2021**, *10*, 434. [CrossRef]

145. Medhane, D.V.; Sangaiah, A.K.; Hossain, M.S.; Muhammad, G.; Wang, J. Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach. *IEEE Internet Things J.* **2020**, *7*, 6143–6149. [CrossRef]
146. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
147. Lewis-Pye, A.; Roughgarden, T. How does blockchain security dictate blockchain implementation? In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Online, 15–19 November 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1006–1019.
148. Rana, S.K.; Kim, H.C.; Pani, S.K.; Rana, S.K.; Joo, M.I.; Rana, A.K.; Aich, S. Blockchain-Based Model to Improve the Performance of the Next-Generation Digital Supply Chain. *Sustainability* **2021**, *13*, 10008. [CrossRef]
149. Sunarya, P.A.; Rahardja, U.; Sunarya, L.; Hardini, M. The Role of Blockchain as A Security Support For Student Profiles In Technology Education Systems. *InfoTekJar J. Nas. Inform. Teknol. Jar.* **2020**, *4*, 203–207.
150. Manogaran, G.; Rawal, B.S.; Saravanan, V.; Kumar, P.M.; Martínez, O.S.; Crespo, R.G.; Krishnamoorthy, S. Blockchain based integrated security measure for reliable service delegation in 6G communication environment. *Comput. Commun.* **2020**, *161*, 248–256. [CrossRef]