Internet of Things Architectures and Applications

Subjects: Engineering, Electrical & Electronic

Contributor: Sharad Sharma

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.

architecture communication protocol enabling technologies interoperability

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.

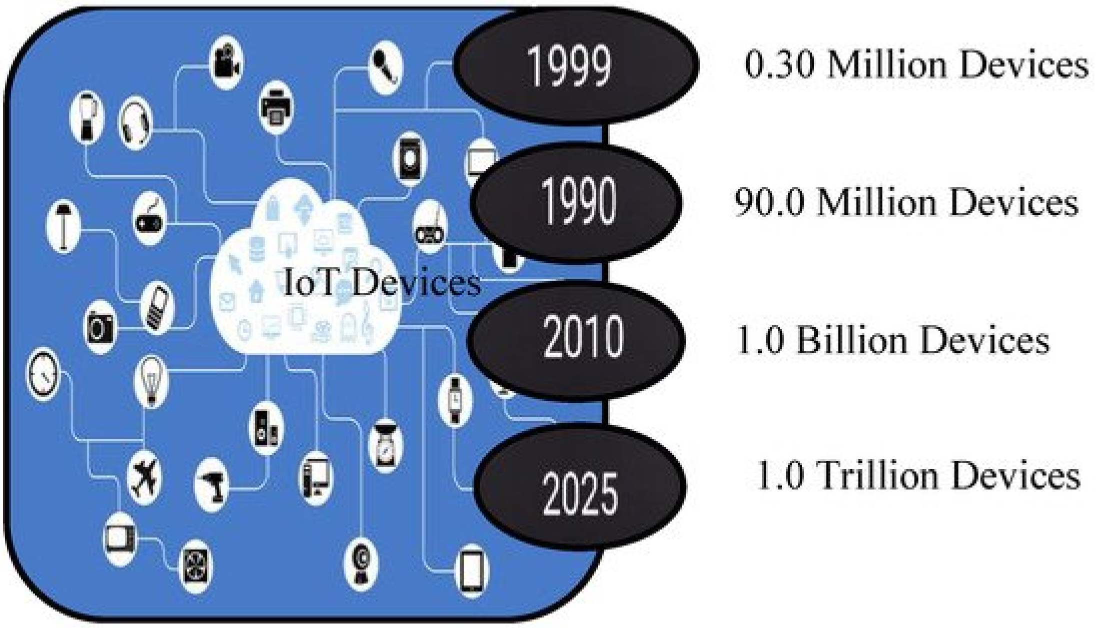

Figure 1. Number of IoT devices till 2025.

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].

2. 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.

2.1. 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 [13]. The IoT design of patented protocols is extremely scalable and can support several different network implementations, as seen in **Figure 1**. 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 2**. It mainly functions on three layers; the function of each layer is discussed below.

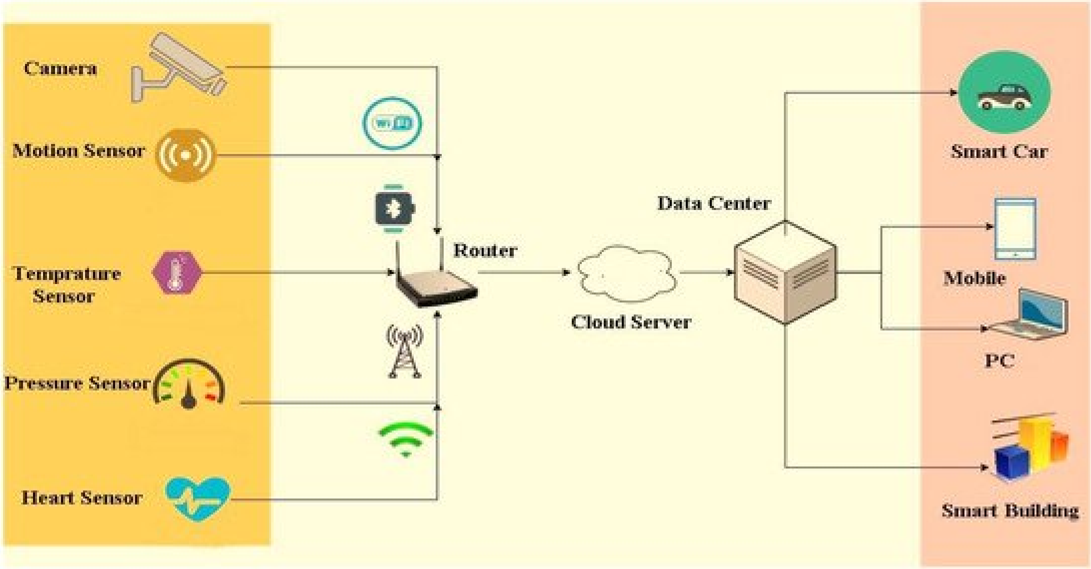

Figure 1. IoT Architecture.

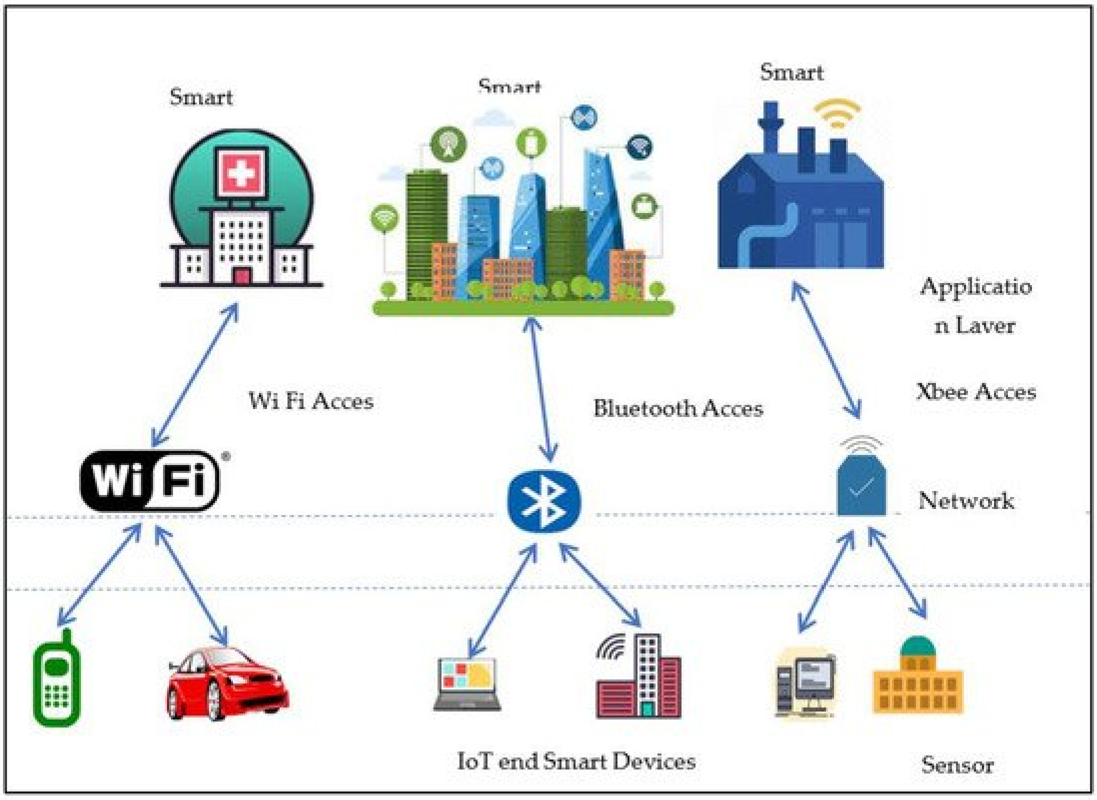

Figure 2. IoT layer architecture.

2.1.1. 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.

2.1.2. 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.

2.1.3. 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.

2.2. IoHT Architecture

The main design challenges for an efficient IoT architecture in a heterogeneous setting are scalability, modularity, interoperability, and flexibility [14]. 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 3, based on IoHT, portrays the information stream across these layers. Because of human association, each layer in [15] 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.

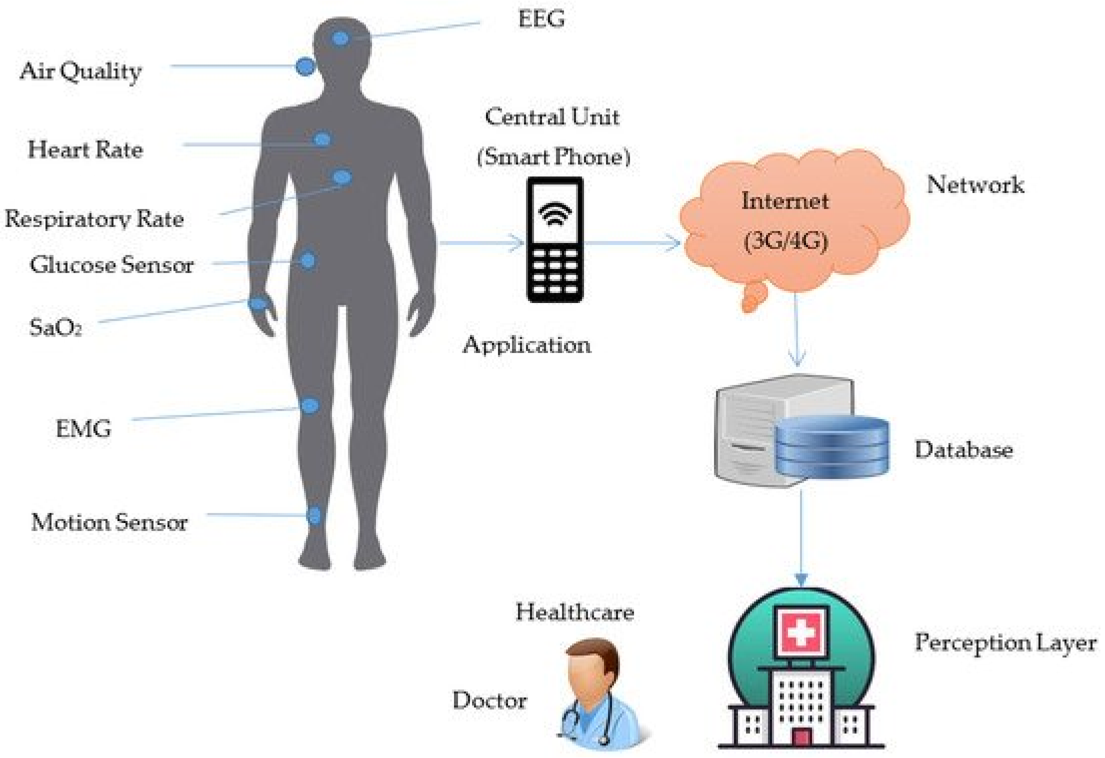

Figure 3. Healthcare models of IoHT.

2.3. 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 4**, 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.

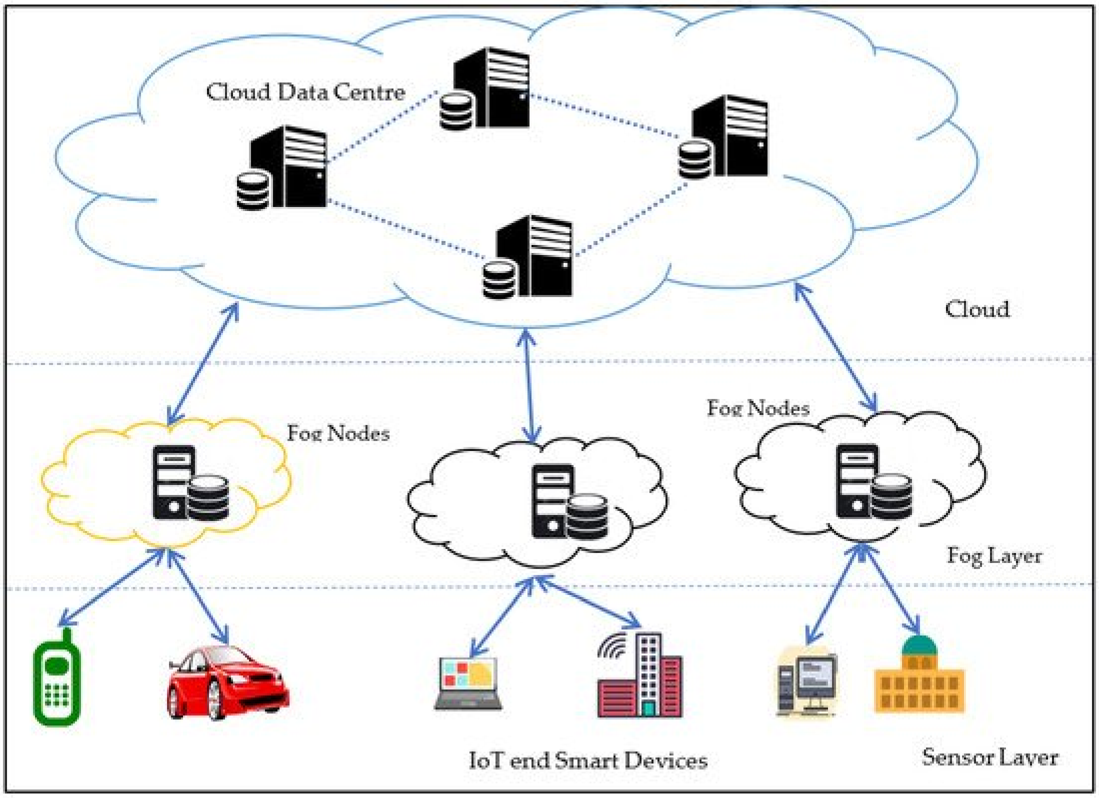

Figure 4. The system architecture of IoT with fog computing.

2.3.1. 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.

2.3.2. 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.

2.3.3. 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.

2.4. 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 5** 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 [16].

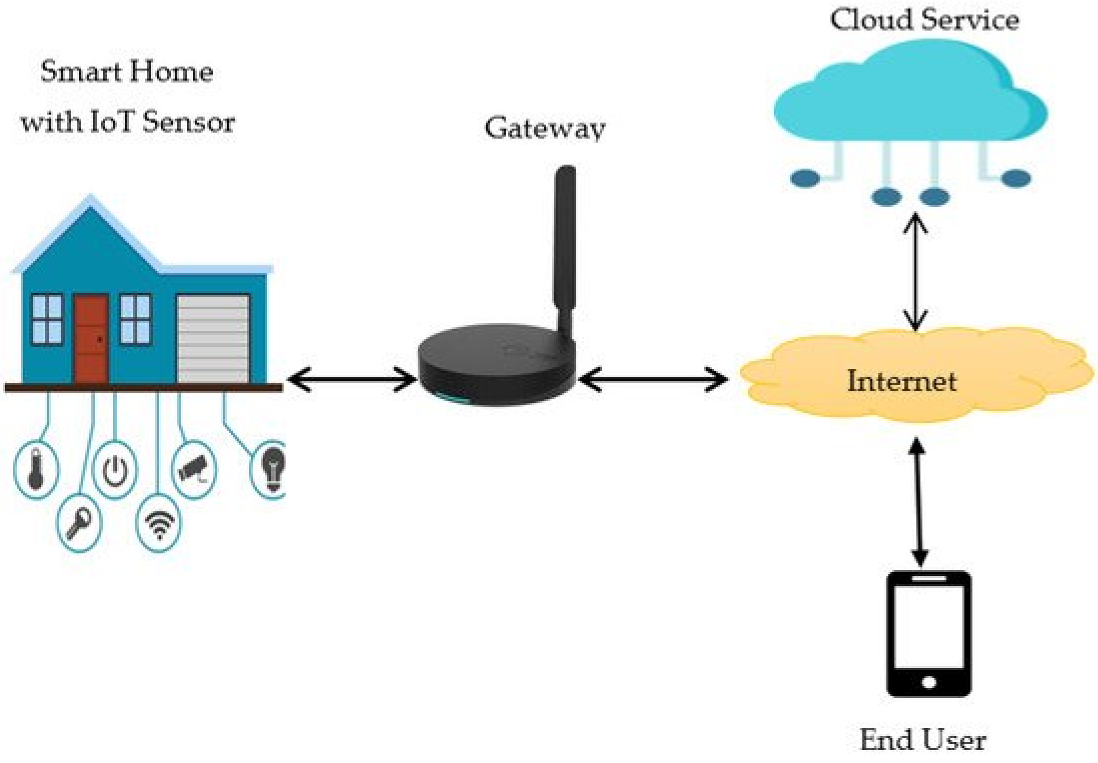

Figure 5. IoT-based smart home architecture.

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.

2.5. 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 [16]. 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 6** 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.

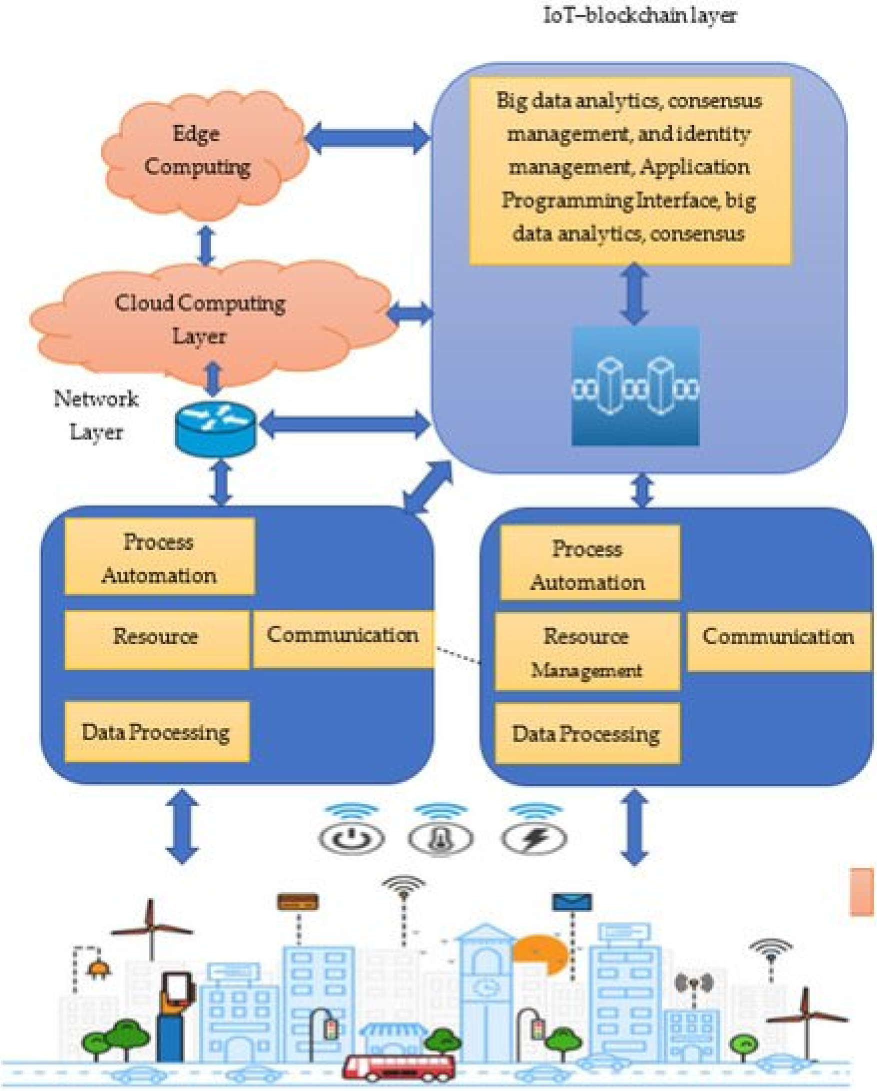

Figure 6. Blockchain-Based Smart City Architecture.

3. 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 7**.

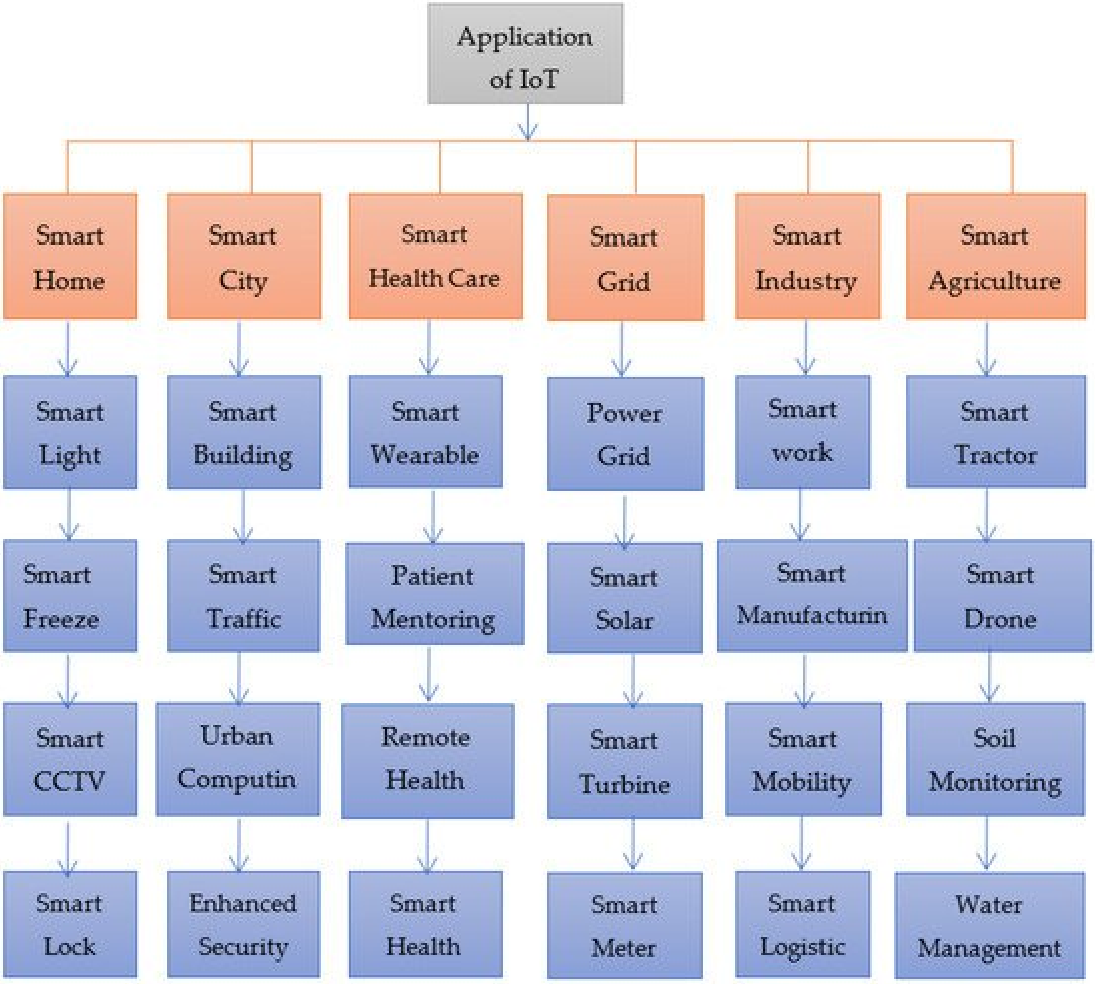

Figure 7. Application domains of IoT.

2.1. 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 [17]. Some smart home features are shown in **Figure 8**.

Figure 8. Smart home features.

3.2. 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 [18]. Some smart agriculture features are shown in **Figure 9**.

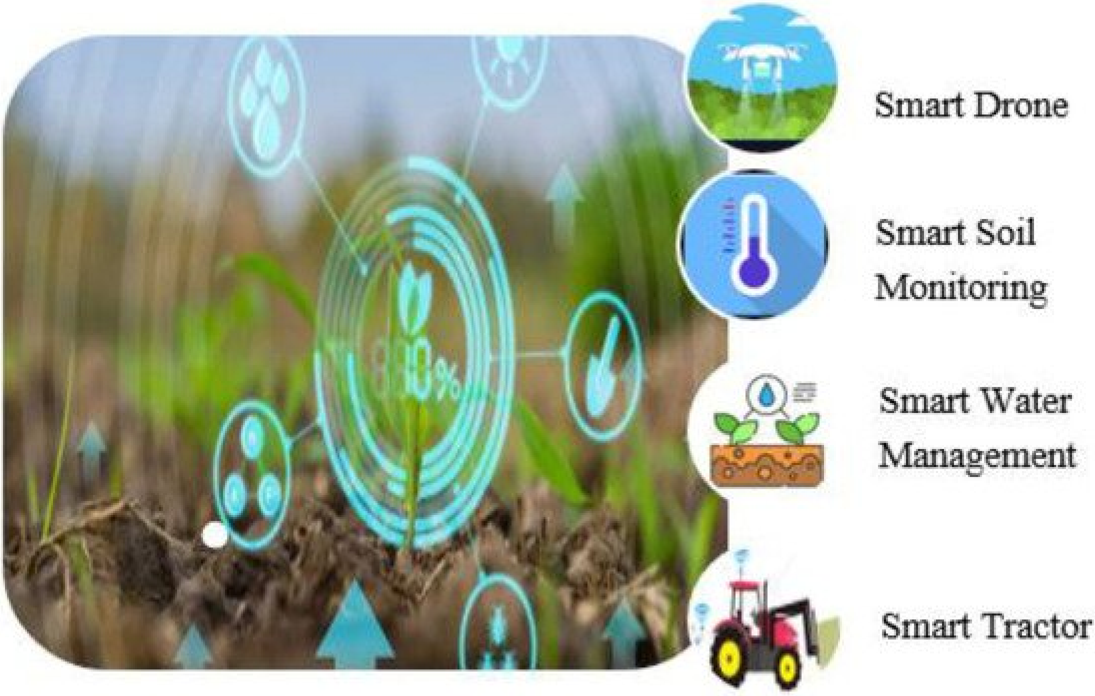

Figure 9. Smart Agriculture Features.

3.3. 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 [19]. Some smart city features are shown in **Figure 10**.

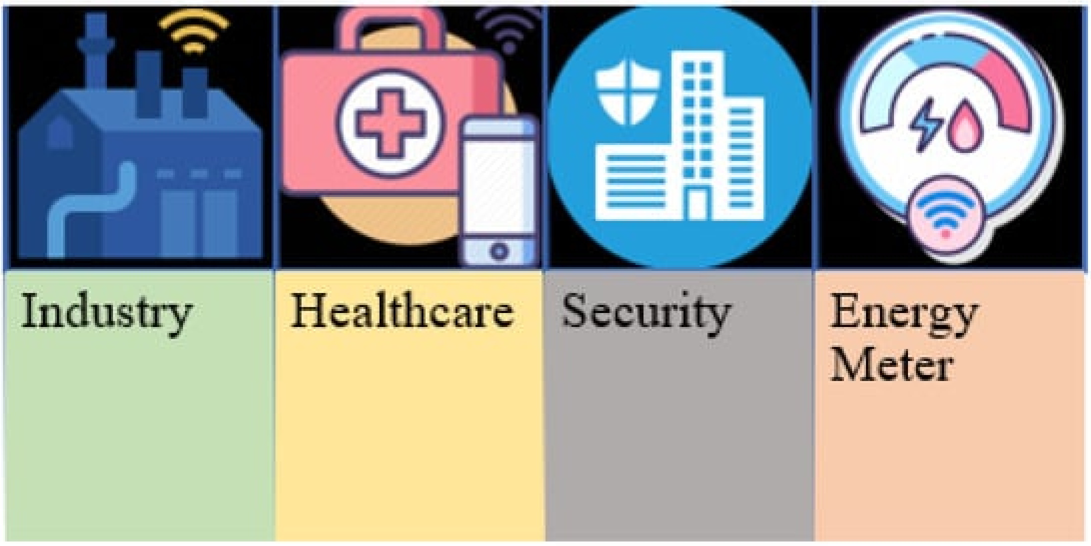

Figure 10. Smart city features.

3.4. 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 [20]. Some smart healthcare features are shown in **Figure 11**.

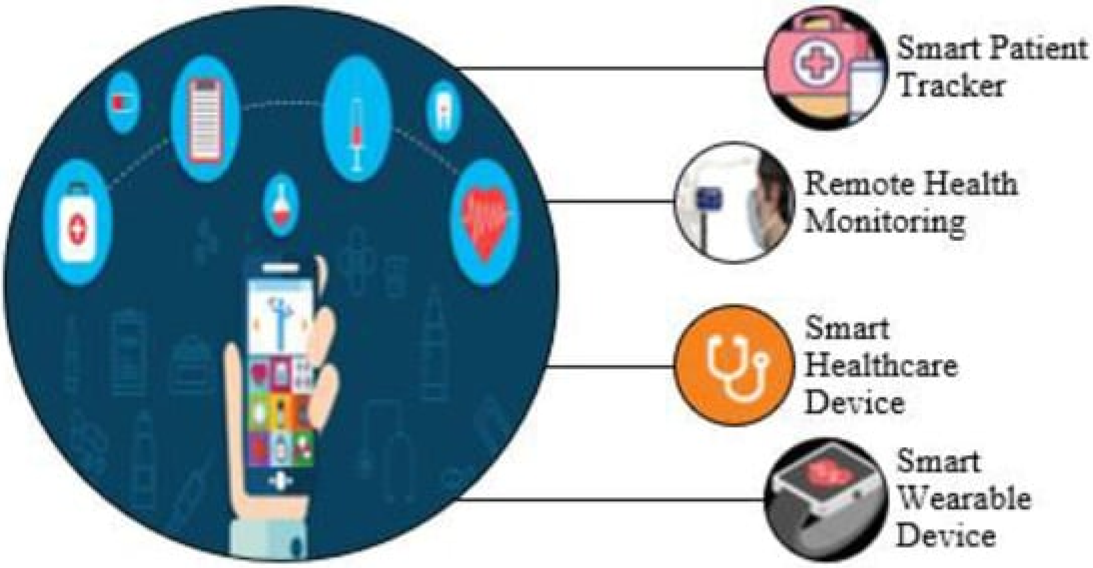

Figure 11. Smart health care.

3.5. 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 [21]. Some smart grid features are shown in **Figure 12.**

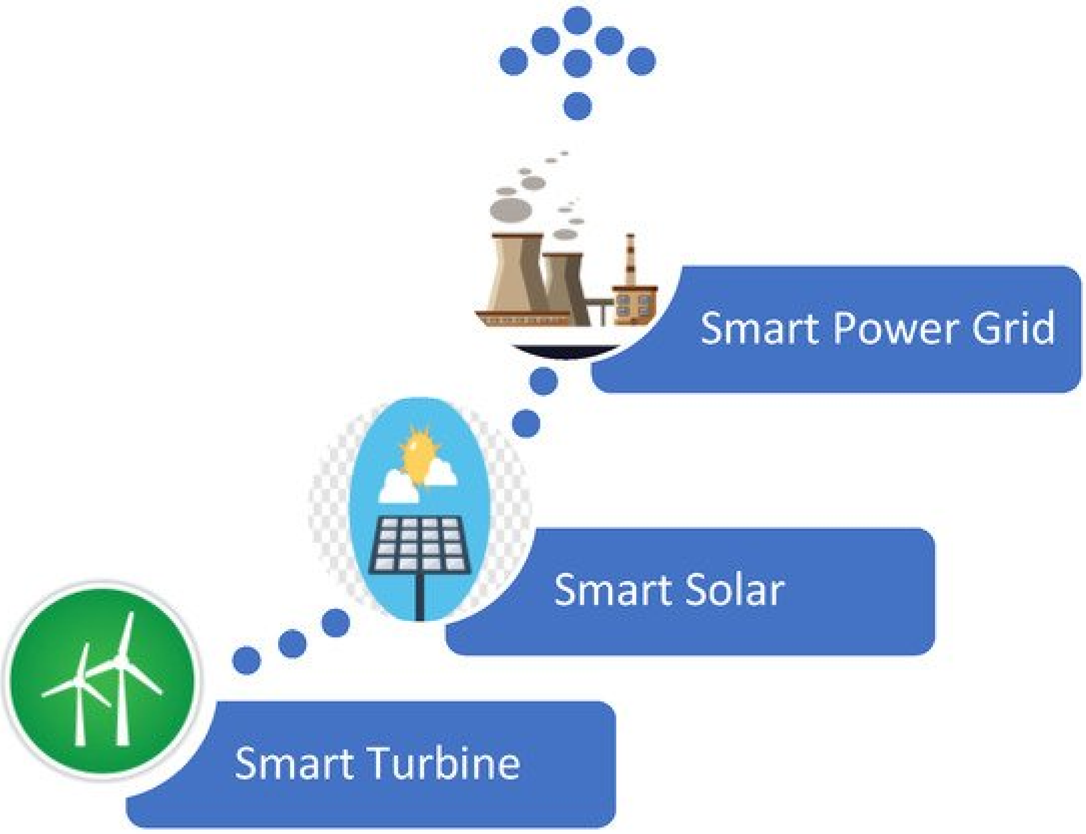

Figure 12. Smart grid features.

3.6. 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 [21]. Some smart industry features are shown in **Figure 13**.

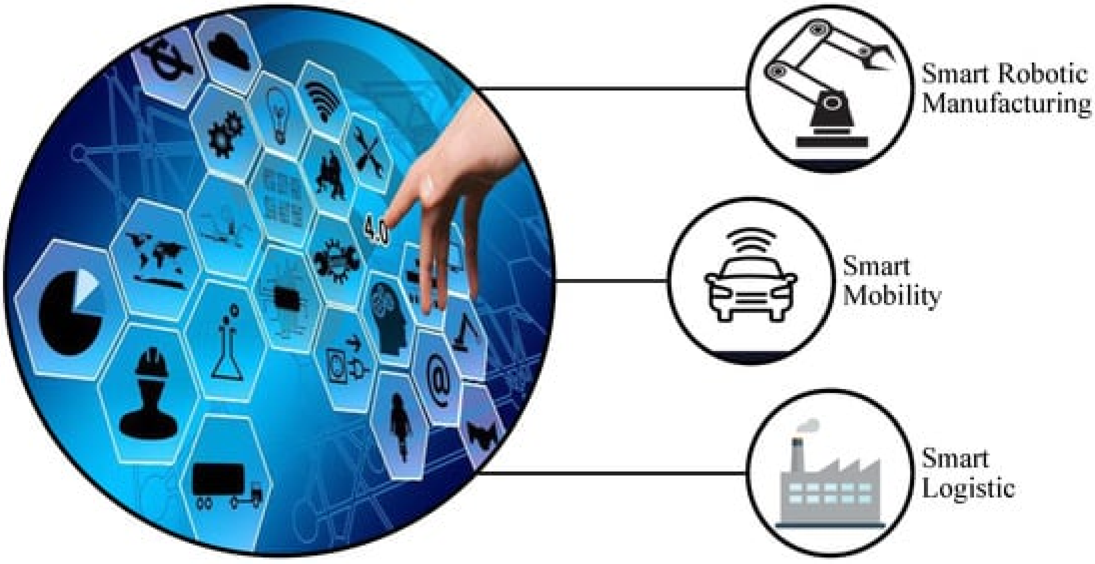

Figure 13. Smart industry features.

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.

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.

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.

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.

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.

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.

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.
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.
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.
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.
13. 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.
14. Sarrab, M.; Alshohoumi, F. Assisted-Fog-Based Framework for IoT-Based Healthcare Data Preservation. Int. J. Cloud Appl. Comput. 2021, 11, 1–6.
15. 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.
16. 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.
17. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-based authentication and authorization for smart city applications. Inf. Process. Manag. 2021, 58, 102468.
18. 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.
19. 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.
20. 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.

21. 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.

Retrieved from https://encyclopedia.pub/entry/history/show/43640