

Article

IoT in Smart Cities: A Survey of Technologies, Practices and Challenges

Abbas Shah Syed ^{1,*}, Daniel Sierra-Sosa ², Anup Kumar ¹ and Adel Elmaghraby ¹

¹ Department of Computer Science and Engineering, University of Louisville, Louisville, KY 40208, USA; anup.kumar@louisville.edu (A.K.); adel.elmaghraby@louisville.edu (A.E.)

² Department of Computer Science and Information Technology, Hood College, Frederick, MD 21701, USA; sierra-sosa@hood.edu

* Correspondence: m0syed03@louisville.edu

Abstract: Internet of Things (IoT) is a system that integrates different devices and technologies, removing the necessity of human intervention. This enables the capacity of having smart (or smarter) cities around the world. By hosting different technologies and allowing interactions between them, the internet of things has spearheaded the development of smart city systems for sustainable living, increased comfort and productivity for citizens. The IoT for Smart Cities has many different domains and draws upon various underlying systems for its operation. In this paper, we provide a holistic coverage of the Internet of Things in Smart Cities. We start by discussing the fundamental components that make up the IoT based Smart City landscape followed by the technologies that enable these domains to exist in terms of architectures utilized, networking technologies used as well as the Artificial Algorithms deployed in IoT based Smart City systems. This is then followed up by a review of the most prevalent practices and applications in various Smart City domains. Lastly, the challenges that deployment of IoT systems for smart cities encounter along with mitigation measures.

Keywords: smart cities; internet of things (IoT); artificial intelligence; sensing technologies; smart city challenges; privacy; security



Citation: Syed, A.S.; Sierra-Sosa, D.; Kumar, A.; Elmaghraby, A. IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. *Smart Cities* **2021**, *4*, 429–475. <https://doi.org/10.3390/smartcities4020024>

Academic Editors: Aneta Poniszewska-Maranda and Witold Maranda

Received: 9 March 2021
Accepted: 23 March 2021
Published: 30 March 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With a bulging world population and increasing urbanization which is set to grow by more than 10% in the next 30 years [1] resulting in a total of 70% living in cities by 2050, countries around the world are looking at equipping their cities to deal with the influx of people and the stress it will bring to current city systems [2]. This is to be carried out keeping in view the UN Sustainable Development Goals 2030 [3]. In this regard, Smart Cities have come out as a major initiative by various governments in making cities more navigable and welcoming to the expected population increase and providing city dwellers a better living experience, as is evidenced by the multiple projects ongoing on both the public and private level [4–7]. In this survey, we provide a review of the use of IoT in Smart Cities and discuss how they facilitate such initiatives. However, since this topic is of high interest to researchers, while conducting the literature search, several surveys were found relating to this topic [8–12]. The authors in [9] discuss challenges that IoT deployment faces in Smart Cities and look at their interrelation based on experts available to them and rank them. Our work is different from [9] in that our coverage of the challenges is blind to specific expert opinion and therefore not limited in scope to their application domain only, we provide an across the board discussion of the critical aspects that IoT designers in Smart Cities need to be vary about and go through practices addressing each of those aspects. The authors in [8] focus their discussion on the architecture and applications of IoT in Smart Cities and briefly describe the technologies used. Surveys in [10,11] provide an application oriented discussion for specific systems which have been developed for various smart city components and follow it up by case studies of cities with active smart

city projects. In [12], the authors discuss the use of big data for cyber physical systems and discuss the different data generation mechanisms, collection, storage, analytics and security as well as steps to move to a greener deployment of such systems. They also talk about various application avenues of such systems. In contrast to the works of [8–12], we provide a detailed overview of the different core units and the technologies used in smart city implementations and discuss the current state of their usage/deployment. Figure 1 provides the structure of the survey. The main contributions of this paper are as follows:

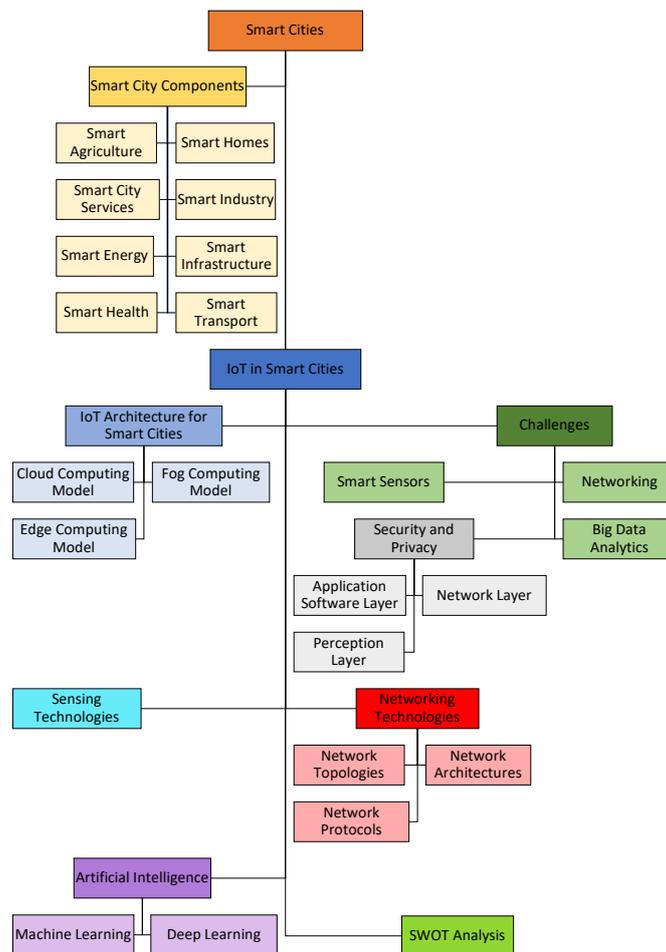


Figure 1. Outline of the survey paper.

1. It lays out the structure of Internet of Things in a Smart City context, discussing its various applications, components and architectures.
2. It provides a comprehensive survey of IoT technologies used at the different levels of the IoT architecture.
3. It provides a discussion of the technical challenges that exist in the deployment of IoT in the Smart City domain and identifies potential solutions to those challenges.
4. It provides insight into current state of IoT usages and discusses different ways in which AI has been applied in the IoT for Smart Cities using the application of clustering, regression, classification etc. In addition, various applications, solutions and data used for implementing the overall framework of Smart Cities are discussed in detail. The discussion includes data sources, algorithms used, tasks performed, and types of deployment used by these proposed approaches.
5. It suggests future recommendations regarding vital aspects of IoT implementation in Smart Cities.

It is hard to define a Smart City, in fact, cities claim to be ‘smart’ based on a variety of criteria, for, e.g., implementing novel e-governance schemes, creating social learning ventures and community engagement programs, focusing on sustainable living as well as the more typical application of Information and Communication Technologies for innovation [13]. In this paper, we define Smart Cities to be the application of various information and communication technologies with the aim of creating a better living experience for a city’s population. This encompasses use of these technologies in all the domains discussed previously, including governance, transport, housing, business, sustainable living, social learning, community engagement, providing opportunities and more. In an ideal sense, the idea of a smart city transcends the typically set boundaries of a traditional city’s administrative and social structure by allowing interaction between the two, thereby enabling it to operate in a more cohesive and engaged manner. Smart cities offer several advantages (in terms of value) compared to a traditional city ecosystem:

1. **Climate goal achievement:** Smart cities are at the forefront of pioneering technologies to help enable countries meet climate goals. Smart city focuses on smart energy management, smart transportation systems and city administration which aim to reduce the carbon footprint of cities and enable development and use of new technologies for cleaner living.
2. **Money value:** Smart City ventures will be a market of USD 1 Trillion by 2025 [14], this provides a huge monetary incentive for not only governments but private companies to actively contribute to the development of technologies supporting smart city development.
3. **Societal impact:** The centerpiece of the smart city project is to improve the quality of life of a city’s inhabitants and help develop an inclusive society wherein every opinion is catered for and equal opportunity is provided. Information and Communication Technologies in the smart city context are a fundamental component to the provision of public services by facilitating interactions of citizens with the city environment and making life easier.

2. Smart City Components

A smart city is made up of several components which are illustrated in Figure 2. Smart city applications typically have four aspects associated with them, the first is the collection of data, the next is its transmission/reception, third is the storage and fourth is analysis. The collection of data is application dependent and has been a real driver for sensor development in the various domains. The second part is the exchange of data, this involves data transmission from the data collection units towards the cloud for storage and analysis. This task has been achieved in several manners, many smart city ventures have city-wide Wi-Fi networks, 4G and 5G technologies are being used, as well as various types of local networks which can convey data either on a local level or a global level. The third stage is storage in the cloud, different storage schemes are used to arrange and organize data so as to make it usable for the fourth stage which is data analysis. Data Analysis refers to the extraction of patterns and inferences from the gathered data to guide decision making. In some situations, simple analysis such as basic decision making and aggregating would work too. For more complex decision making, the availability of the cloud allows not only for heterogeneous data gathering/storage and processing but also analysis through the use of statistical methods as well as machine and Deep Learning algorithms in real-time [15].

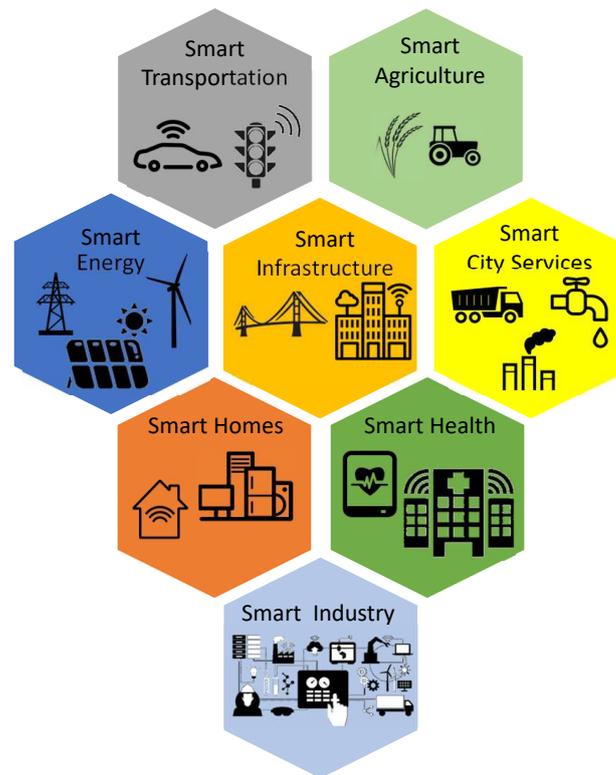


Figure 2. Smart City Components.

2.1. Smart Agriculture

Food security is one of the most important parts of the United Nations Sustainable Development goals for 2030. With an increasing world population, worsening climate change causing erratic weather in food centers of the world, the race to ensure that food production is made sustainable and that dwindling resources such as water are utilized efficiently has been a high priority for countries around the world. Smart agriculture is the use of sensors embedded into plants and fields to measure various parameters to help in decision making and prevent/diseases, pests etc. [16]. A part of the smart agriculture paradigm is precision agriculture, which involves sensors being placed in plants to provide targeted measurements and therefore allow for targeted care mechanisms to be deployed. Precision agriculture will be necessary for food security in the future [17] and therefore is an essential part of the fight for sustainable food production. The major applications of AI in IoT for agriculture are crop monitoring/disease detection and data driven crop care and decision making.

2.2. Smart City Services

Smart city services encompass the activities that sustain a city's population, these involve municipal tasks such as supply of water, waste management, environmental control and monitoring etc. Sensors for water quality can be deployed to continually provide an update about the quality of water being used in the city and detect leaks [18]. One popular component of smart city initiatives is the management of waste, and it has been the part of many of the smart city initiatives mentioned earlier, from chutes in Barcelona to having bins equipped with sensors and connected to the cloud so as to not only inform the relevant authorities of the need to empty them but also using AI to determine the best route to reduce cost [19]. Sensors can also be used to monitor the environmental conditions in a city to determine pollution levels [20] and guiding citizens to the next free parking space to save fuel costs [21].

2.3. Smart Energy

Typical electrical systems have one-way energy flow from a main generator source, usually a hydroelectric or fossil fuel based power plant. Power generation is controlled via feedback from the substations, however, since there is no information feedback from the consumer end, the power generation scheme used with these systems requires that the power being produced by these sources outstrips the demand by a large amount to ensure continuous supply of power. The process of detecting faults and performing corrective actions in such systems is also a time taking process. Moreover, with renewable energy technologies becoming cheaper, the consumer of today not only has a supply from the main utility but also performs their own generation. Smart Grids is the use of ICT technologies to make the current and newly installed grids more observable, allow for distributed energy generation, both at the consumer end as well as the utility end and introduce self-healing capabilities in to the grid. One aspect of smart grids is that real time power data is transmitted to utilities at different points on the grid throughout the supply lines till the customer. Since smart grids provide real-time data about consumer usage, it allows for better management of power generation using prediction models developed through acquired consumption data, integrating different energy sources as well as self-healing [22] of the network to ensure an uninterrupted supply.

2.4. Smart Health

Smart Health refers to the use of ICT to improve health care availability and quality. With an increasing population and rising costs of healthcare, this area has been of intense focus of researchers as well as healthcare providers. Current health systems are over burdened and therefore cannot cater to the increasing demand from the populace. In this regard, smart health aims to ensure that healthcare be available to as many people as possible through telemedicine services [23] and improved diagnosis assistance to doctors utilizing AI [24]. With the ubiquitousness of mobile phones and health trackers [25] that can capture real-time data about peoples health (ECGs, temperature, body oxygen saturation and other biosensors) while also recording daily activity and detecting abnormal movements using inertial sensors, it has become possible to leverage cloud capabilities for processing this data to make better healthcare decisions. Thus, reducing the overall costs as well as burden on healthcare facilities.

2.5. Smart Home

One major component of Smart Cities is the Smart Home since it is the central to the life of the city's inhabitants. Smart Homes involve the use of sensing units installed throughout a person's home that provide information about the home as well as its occupants. These sensors might include user activity monitors such as ambient sensors, motion trackers and power/energy consumption.

2.6. Smart Industry

Industries around the world are busy in a continuous pursuance of being more efficient and increasing productivity while reducing cost. The industry 4.0 paradigm entails the vision of a connected factory where all its intermediary functionalities are seamlessly integrated, working in tandem with each other. This is made possible because of the internet of things [26]. The use of IoT in manufacturing and production processes, cyber physical systems integrating workers and machines has led to several benefits to the industry such as faster and better innovation, optimization of manufacturing schemes (resources and processes), better quality of products and enhanced safety for factory workers. However, smart industries come with several challenges for IoT usage, working with a set of heterogeneous devices and machines has its own challenges and requires cyber physical systems to have flexibility in configuration, connectivity and quick implementation for use in IoT applications for Smart Industry [27]. Artificial Intelligence has gone hand in hand with IoT to spur the development and deployment of industry 4.0 services. With

sensors being embedded in machines and other processes in the factory, data from these sources provide an opportunity for using AI techniques to increase automation, perform business intelligence operations and more. In fact, researchers have suggested frameworks for integrating AI within IoT for Smart Industry [27–29]. The major applications of AI in the industry are predictive maintenance, monitoring/fault detection (machine health) and production management.

2.7. Smart Infrastructure

The infrastructure of a city is paramount to its living quality, city governments need to construct new bridges, roads and buildings for the use of its inhabitants and also perform maintenance for uninterrupted usage. Smart infrastructure helps cities in ensuring their infrastructure is in shape and usable by utilizing sensors for measuring building/bridge structural state for structural health monitoring using accelerometers [30] and smart materials [31]. Data collected through these sensors allows for predictive maintenance of these essential units to maintain normal operation of the city.

2.8. Smart Transport

Many urban centers suffer from traffic problems, this includes congestion, pollution, scheduling and cost reduction issues for public transport. The rapid development and implementation of new Information and Communication Technologies, Vehicle-Infrastructure-Pedestrian communication has become commonplace. Whether it be Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrian (V2P) or Pedestrian to Infrastructure (P2I), such technologies have made the design of smart transportation systems possible. With cars having a GPS device and the commonality of cellphones with every driver, many approaches use GPS data to track driver behavior and traffic patterns [32]. This real-time data is already used for route mapping in applications such as Waze and Google Maps and used for trip scheduling in public transport. Parking systems equipped with sensors can also guide drivers to the nearest free parking spot.

3. Internet of Things for Smart Cities

At the heart of the Smart city initiatives is the internet of things (IoT), it is the enabling technology that has allowed for the pervasive digitization that gives rise to the concept of smart cities. The internet of things refers to the ubiquitous connection of devices to the internet, allowing them to send information to the cloud and potentially get directions for performing actions. IoT involves the collection of data and performing data analytics operations to extract information in order to support decision and policy making. It is estimated that by 2025 more than 75 billion devices will be connected to the internet [33], spearheading even more application development. Within the smart city context, IoT allows for sensors to collect and send data about the city's state to a central cloud, which is then mined or processed for pattern extraction and decision-making purposes.

3.1. Iot Architectures for Smart cities

The Internet of Things unifies the operations of data sensing, transmission/reception, processing and storage through the use cloud services. Based on technology, a generic IoT architecture consists of five layers where successive layers operate on the information from the previous layer as shown in Figure 3. It also shows the three different architectures that exist for IoT systems.

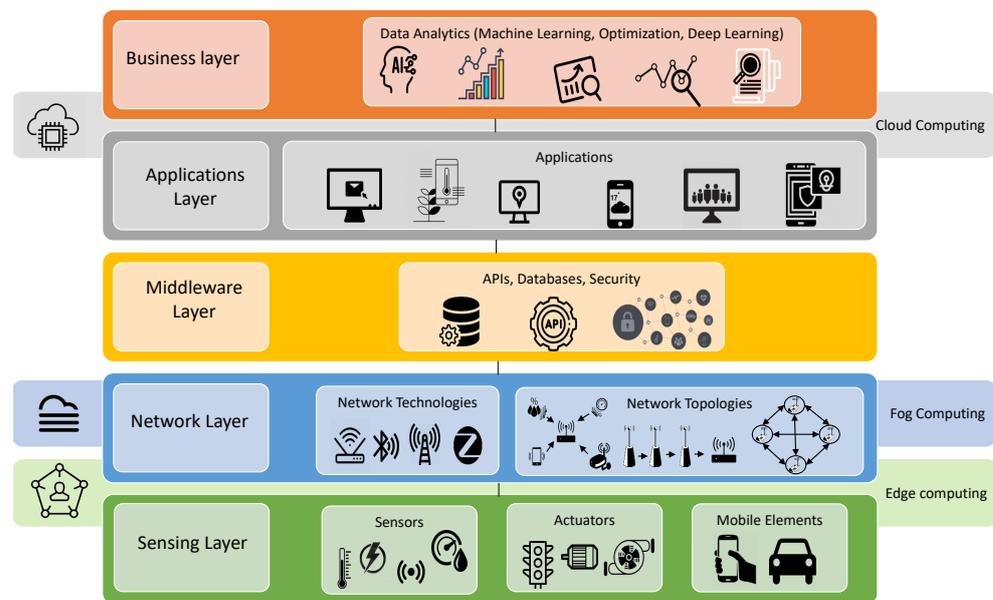


Figure 3. IoT Architecture.

The Sensing layer, also called the Perception layer consists of sensors that can get information about physical quantities of interest in any application as well as actuators which can act upon physical objects, such as RFID readers for reading RFID tags and other such devices. The data read by the sensing layer is passed onward to the Middleware layer using the networking layer through wireless network technologies such as Wi-Fi, cellular internet, Zigbee and Bluetooth etc. The Middleware layer provides a generic interface for the sensing layer hardware and the Application layer which uses the data through various API’s and database management services to provide users with services. The Business layer is attached to the application layer and is used to develop strategies and formulate policies that help manage the complete system.

In terms of architectures, typically, IoT architectures are categorized based on the type of operation responsibilities allocated to parts of the IoT system, this categorization is based mainly on processing of data responsibilities. There are three architectures of IoT systems with respect to the stage of the IoT framework where processing of data can be carried out and these are Cloud, Fog and Edge Models. Table 1 lists the traits of each of three layers of the IoT system. It is important to mention that the three IoT architectures discussed here are not mutually exclusive, instead the aim of this hierarchy is to complement the higher layer by providing it only useful information which makes the system more productive and dependable. For any IoT system designer, the aim is to establish a balance between the capabilities of the three layers keeping in view system costs and requirements.

Table 1. Comparison of Cloud, Fog and Edge Computing Models.

Cloud Computing Model	Fog Computing Model	Edge Computing Model
Contextual awareness on a global level encompassing all aspects of the application	The Fog layer has contextual awareness of the local sensing scenario	Edge devices typically only have information about their own status. Exchange strategy possible but limited to local neighborhood
Farthest away from the edge and therefore decision making can be slow and latency is high	Being the closest unit to the edge, the Fog layer can respond much more quickly to the data being sent from sensors and other devices, as it can aggregate the information sent	Quickest decision making possible; however, decisions will be based on local states

Table 1. Cont.

Cloud Computing Model	Fog Computing Model	Edge Computing Model
Utilizes heterogeneous data from a variety of sensing devices	Utilizes heterogeneous data, but within a small region	Usually do not have access to different types of data
High network cost	Medium network cost as data flow is reduced	Least network cost
Potential privacy risk as raw data might be sent to the Cloud	Increased privacy compared to Cloud computing	Even greater privacy enforcement possible than Fog computing model
Least robust as decision making is centralized	More robust than Cloud computing model	Most robust as distributed decision making takes place
Best capabilities in terms of resources	Lesser capable than Cloud devices	Least capable
Scalability is low	Scalability is better than Cloud	Scalability is highest

3.1.1. Cloud Computing Model

This was the first proposed architecture for IoT systems and is based on the premise that processing of data from the various components in the IoT system should take place in the cloud. Cloud computing allows for the remote accessing of uninterrupted shared resources (computing, storage and services) over the network. It should be able to dynamically allocate these resources without human intervention, schedule or pool as necessary and be able to be accessed from a variety of different platforms [34]. The cloud can provide both hardware as well as software services for smart city applications. It has the advantage that it provides a central management platform from which to observe, control the IoT system as well as to disseminate command actions based on the received data. Moreover, this centralization also allows for cloud systems to have sufficiently large computing and storage capacities thereby allowing them to perform complex tasks of data mining, pattern extraction and making inferences from sensor data in smart cities to make use of it in the best manner possible. However, there are a few disadvantages with using the cloud computing model for the IoT. First, transmitting all gathered data to the cloud increases network traffic, even though this may not be true for applications in which measurements are not very frequent, but in other cases, this could increase network costs. Moreover, data transmission overheads may increase due to the large amount of data that needs to be transmitted by the many sensors existing in the smart city scenario. Another disadvantage that the cloud computing model suffers from is data latency, since the sensing units exist at the sensing layer and the decision making/data processing takes place in the cloud, this gives rise to data latency in the transmission of sensing information, especially when many devices start sending data at the same time. Network reliability can be an issue when using this model, with the large volume of data traffic on the network, it might not be possible to enforce robust data transmission schemes as IoT systems get bigger.

3.1.2. Fog Computing Model

Since most of the information produced with in IoT takes place towards the sensing end of the IoT system, also called the edge, Fog Computing was proposed in [35] to overcome some of the problems of the cloud computing model for the IoT. Fog computing provides a more diverse distribution of responsibilities than are dictated by the cloud computing architecture by moving some of the processing to devices on the local network. Typically, Fog computing refers to data processing that is carried out by routers and other network devices within in the Network layer in the IoT. Since network devices nowadays increasingly offer better computational capabilities, one can leverage them to perform rudimentary operations on data. Operations such as aggregation and collection of sensor data, simple processing operations and decision-making can be performed to reduce the amount of information flow towards the higher cloud layer. Questions that need to be answered for the decision-making process include but are not limited to for, e.g., does the decision require the use of averaging for one quantity and instantaneous values of the

other? Is it possible to extrapolate data received for one quantity and use the currently measured value for another one? Based on the previous data for a given period, can one provide higher layers with decision options rather than just data, thereby providing better quality information to the cloud layer thus resulting in better utilization of cloud resources. Fog layers can localize decision making since they have access to the local state of a given region [36]. This would be helpful in implementing distributed decision making mechanisms which might be necessary in some applications. Moreover, they also allow for local networks to be established using non-internet technologies such as Zigbee, Bluetooth, RFID etc. where sensors and other end devices transmit data to the Fog node (also referred to as access points in such systems) which is connected to the cloud.

Fog computing results in reduced costs for deployment of IoT systems, increases robustness as latency, data overhead and errors in transmission are reduced. This also improves the efficiency of the applications as quicker decisions can be made on the received data, which is important in critical decision-making situations. Moreover, Fog devices have the capability to not only receive data from similar devices at the edge but also collect it from many different types of devices. This capability to measure different parameters in the edge environment enable for an application neutral IoT system architecture to be developed.

Data sent upward by the Fog layer in the IoT hierarchy would be used to gain insights in to system behavior and to guide new rules of system operation, this will typically be carried out in the cloud. Devices in the Fog layer may be provided decision making guidance from the higher cloud layer to ensure smooth system operation. However, a balance needs to be struck as to the division of responsibilities between the cloud and the fog layer keeping in view the costs involved.

3.1.3. Edge Computing Model

The purpose of Fog Computing was to push some of the decision making towards the edge of the network. In recent years, with increasingly capable devices being developed that are attached to 'edge' nodes, simple decision making, and processing of data has been increasingly moved on to these devices so as to reduce network and device costs even further at the fog level and make for even deeper distributed decision-making schemes. Edge computing refers to data processing that is done at the "thing" level, i.e., by sensors and other devices in the IoT system [37]. Another concept about Edge computing as discussed in [38] defines the Edge computing layer as an intermediary layer between the Fog and the 'things' (sensors) rather than edge nodes. The difference between them in this case is the Edge computing nodes act as aggregation and decision-making units on a smaller scale compared to fog devices which act to provide seamless connectivity and data integrity throughout the IoT network. The aim of the Fog and the Edge computing paradigms is to decentralize the IoT system for purposes of reducing cost, increasing scalability and increasing robustness.

3.2. IoT Challenges for Smart Cities

The Internet of Things promises the digitization of all aspects of our lives. For smart cities, this digitization process entails the proliferation of sensing nodes in every domain of a city's operation mechanism. With an application scope this broad, the creation and subsequent deployment of IoT systems in smart cities carry enormous challenges that need to be considered. In this section, we provide a discussion of the challenges that IoT system designers face when making deployments in smart city applications. In this paper, we focus on the technological challenges that pertain to IoT use in smart cities and have been the focus of researchers. Figure 4 shows the different challenges which Smart City IoT system deployment encounters, namely Security and Privacy, Smart Sensors, Networking and Big Data Analytics. A summary of the discussion in this section is presented in Table 2.

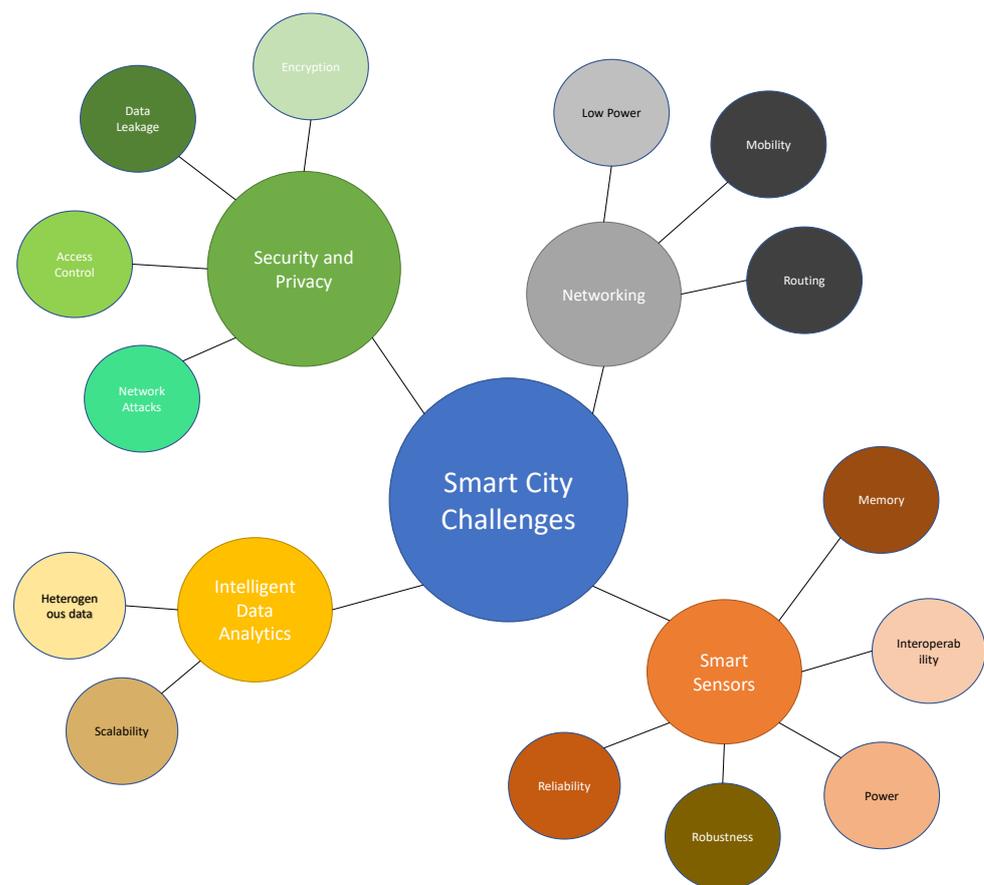


Figure 4. Challenges for IoT in Smart Cities.

3.2.1. Security and Privacy

Security, along with Privacy is the primary concern in smart cities. Smart cities involve having essential city infrastructures online, any aberration in the operation of the city's services will bring inconvenience to its citizens and put human lives and property at risk. Therefore, security is a big concern in smart cities. In today's age where cybercrime and warfare have become a tactic in world politics, smart cities are at an ever-greater risk of being the target of such malicious attacks. Encryption of data transmitted over the network is necessary in this scenario. For smart city projects to be successful, they require the trust and participation of citizens. The proliferation of sensors in smart cities, which continuously collect data about the activity of people may expose the daily activities of citizens to unwanted parties. Moreover, companies and corporations on the IoT network may use citizen data without their approval for things like targeted advertising and may perform acts such as eavesdropping etc. Solutions to this will require processes that anonymize data collection while retaining the integrity of the context of the measured task so that apt decision making is possible. Security and Privacy has been covered in detail in this paper.

3.2.2. Smart Sensors

Smart sensors are the hardware components that gather data in smart cities. These devices are manufactured by a host of different vendors that adhere to different sensing mechanisms, standards of measurement, data formats and connectivity protocols. Smart city deployment will require all these devices to exchange data, perform scheduling of tasks between them and be able to aggregate data together for making inferences. A solution to this issue is to develop and use open protocols and data formats that will enable manufacturers to create equipment that can communicate between each other, further spurring IoT system deployment. Another solution could be the development

of 'standard' access point nodes for IoT systems that can communicate to devices using several different communication protocols and are able to decode the information received. Some manufacturers have, in fact, made their products compatible with other protocols as mentioned in [39].

Another challenge for smart sensors is reliability and robustness. Reliability and robustness refer to the dependability and correctness of the IoT system. IoT is the backbone of future smart cities and being imperative to their operation, the IoT system needs to provide a smooth experience to its users. This requires that service requests from users of the application receive an accurate and timely response. The quality of service needs to be ensured for every citizen in the smart city. Systems that deliver critical utilities such as transport, electricity etc. should be decentralized. The distributed connection points will allow for robustness and increase reliability. One such example is self-healing in Smart Grids [22].

Many current networking protocols are developed for infrastructure networked devices which have access to continuous power, however, sensors in smart cities will be mobile in many scenarios and thus be battery powered. Moreover, they will need to measure, transfer and in some cases save data they have collected. This requires the development of not only low power, low overhead data transmission schemes but also development of new memory and storage technologies as well as low power devices that extend battery life as much as possible. Storing this large amount of data would require development of compression algorithms which will be employed and database schemes that will need to be developed in the future as smart cities and IoT are scaled up. Solutions for power issues necessitate the development of new battery technologies and perhaps the incorporation of energy harvesting mechanisms in such devices to make long lasting service provision possible.

3.2.3. Networking

The IoT depends on the capability of sensing and other devices to be able to send and receive information to each other and the Cloud. With new smart city applications coming up, providing networking to these devices to remain connected is a big challenge. Current networking methods are not optimized to providing networking services for smart city components. Many devices in smart cities have mobility and data throughput requirements which need to be met to provide an acceptable quality of service. Different approaches have been suggested in terms of defining access points, local networks etc. to solve this problem. Another aspect of networking would be working on efficient and dynamic routing protocols that can serve IoT requirements capable of working with stationary as well as devices in motion, which many current protocols do not offer sufficiently [40].

3.2.4. Big Data Analytics

IoT connected devices generated 13.6 Zetta Bytes of data in 2018 and this is expected to grow to 79.4 Zetta Bytes till 2025 [33]. To make use of this data and continuously improve the services that are delivered in smart cities, new data analytics algorithms need to be developed. With the myriad of the different parameters that are measured in smart cities, these algorithms need to be applicable to data of varying nature (both structured and unstructured), better data fusion techniques need to be developed as well so as to combine them in meaningful ways and be able to extract inferences and recognize patterns. Deep learning has been of interest in this area as it can leverage on this large amount of data to provide better results for different applications. Another important consideration would be to ensure that the developed algorithms are scalable in that they have enough generality and can be used through out the intended application. For, e.g., for the purposes of activity recognition, the authors in [41] found that a CNN trained for activity recognition on one dataset failed to perform well on others or in [42] where the deep learning network performs poorly when the color of tomatoes is different from what it was trained on. Concept drift is another issue of concern as with the continuous

acquisition of data, the properties of data may change over time. Techniques such as incremental learning may be useful in this respect. Explainability is another important factor for Smart City analytics to be widely acceptable, specially in the area of smart health. There have been some approaches suggested towards this end, in [43] a hybrid deep learning classifier and semantic web technologies based solution is demonstrated for the application of flood monitoring. In [44], the authors present an explainable deep learning based healthcare system at the Edge for COVID-19 care based on a distributed learning paradigm with promising results. However, more work needs to be performed to incorporate explainability techniques such as distillation, visualization, and intrinsic methods into Machine and Deep Learning based smart city applications in order to increase smart city application proliferation.

Table 2. Smart City IoT Challenges and Mitigation.

Challenge	Mitigation/Research Direction	References
Security and Privacy	Encryption New authentication mechanisms New standards to anonymize data Prevent data leakage	[8–11,45–47] [48–50]
Smart Sensors	Interoperability: Open Standards Reliability and Robustness: Decentralized and distributed architectures and decision making Power and Memory: Energy harvesting, Low power sensors, New database storage systems	[9–11,47–50] [51]
Networking	Low power networks, Network schemes that ensure fluent mobility and routing	[40,47]
Big data analytics	New algorithms which work with different natured data, Develop scalable and explainable AI	[10,47,52]

3.3. Sensing Technologies

Sensing is at the heart of smart city technologies. Sensors provide the knowledge and data from which smart city innovations are created. With the vastly different nature of Smart City projects and its various components, there are numerous sensors which are used as part of these initiatives. The authors in [53] have provided a framework for the comparison of IoT sensors and have listed sensors they found in use for Internet of Things. We use their work to direct our survey of the sensing technologies used in smart cities. Sensors within IoT can be divided in to several groups, these are ambient, motion, electric, biosensors, identification, presence, hydraulic and chemical sensors as shown in Figure 5. Sensors are the key component in smart city IoT systems which provide the interaction between the smart city system and the city's inhabitants and allow for new services to be developed. One thing to note is that many of the sensors find applications in multiple areas as discussed. Furthermore, any given application will require measuring different physical quantities and will require the use of many different types of sensors. For, e.g., ambient, motion, electric, identification, position, chemical and hydraulic sensors have been found to be used in smart homes. As noted in the challenges, working with different sensors which might have different output data types is a task that needs to be dealt with when working with multiple types of sensors. Table 3 presents a summary of the sensors used in each smart city component.



Figure 5. Sensing Technologies for IoT Smart Cities.

3.3.1. Ambient Sensors

Ambient sensors include sensors used to measure physical quantities indicating to environmental conditions such as temperature, humidity, light intensity and pressure. Ambient sensors are used in a variety of smart city applications including smart homes where they are used to regulate the comfort level, they are also used for smart city services.

3.3.2. Bio Sensors

Biosensors are used for measuring health parameters of living things. Biosensors in smart cities are used for monitoring patients for healthcare purposes. Such sensors include ElectroEncepheloGram (EEG), ElectroMyoGram (EMG), ElectroCardioGram (ECG), skin resistance, heart beat, breath sensors, pulse oximetry, blood pressure and more.

3.3.3. Chemical

Chemical sensors are used to measure chemical properties of materials, this includes gas sensors which can measure/detect carbon monoxide (CO), carbon dioxide (CO₂) and other gases for air quality monitoring, sensors for detecting smoke, pH and other sensors for water quality monitoring etc.

3.3.4. Electric Sensors

Electric sensors allow for the measurement of electrical power and are widely used in smart grids and smart homes to monitor the power consumption of consumers/appliances. Types include current transformers and voltage sensors to measure current and voltage, respectively.

3.3.5. Hydraulic

Hydraulic sensors refer to sensors used for liquid measurements such as level, flow, leak detection. These are used for measurement of liquid levels in tanks [54].

3.3.6. Identification

Identification sensors refer to RFID tags and Near Field Communication (NFC) devices. These sensors are used in applications involving payments, data exchange in the domain of smart transportation and smart city services.

3.3.7. Motion Sensors

Motion sensors refer to sensors that can be used for the detection of motion. Sensors for motion sensing involve inertial sensors such as accelerometers and gyroscopes. These sensors are used in smart health applications such as activity tracking as well as applications like vibration sensing in smart homes and industry.

3.3.8. Presence

Presence sensors indicate to the presence of a humans or objects. Passive InfraRed (PIR) sensors are very popular and are used to detect human motion, reed switches can be used on windows and doors for security purposes, inductive loop sensors which use electromagnetic induction can be used to detect presence in transport systems. Ultrasonic sensors are also used to determine the distance of objects. Capacitive sensors are also included in this type, these may be used to determine position.

3.3.9. Other Sensors

Various smart city applications make use of different sensing modalities such as audio or visual information or other signal measurement devices, for, e.g., bluetooth and Wi-Fi signal strength. Since the sensors for these modalities capture raw information about signals (visual, sound or signal strength etc.), the gathered data is typically processed further before it indicates to the target variable being measured.

Table 3. Sensing Technologies for IoT Smart Cities by Smart City Component.

Smart City Component	Sensor Type	References
Smart Agriculture	Ambient, Chemical, Hydraulic, Other sensors	
Smart City Services	Ambient, Chemical, Hydraulic, Presence, Other sensors,	[55–57]
Smart Energy	Ambient, Electric, Motion	[58,59]
Smart Health	Biosensors, Identification, Motion, Other sensors	[60–62]
Smart Home	Ambient, Chemical, Electric, Hydraulic, Identification, Motion, Presence, Other sensors,	[58,63]
Smart Industry	Ambient, Biosensors, Electric, Hydraulic, Identification., Motion, Other sensors	
Smart Infrastructure	Ambient, Motion, Electric, Other sensors,	[55]
Smart Transportation	Ambient, Chemical, Identification, Motion, Presence, Other sensors	[64–66]

3.4. Networking Technologies

The internet of things in smart cities depends on the aggregation of data measured by individual sensing units placed throughout the smart city environment. Systems that can use these measurements individually have long existed and provided automation for small projects. However, the ‘smart’ in smart city comes from the collective usage of the data from these individual sensing units to perform complex decisions while delivering services to citizens. The collective use of this data enables its analysis over a wider scope compared to individual levels so as to determine long term patterns and provide meaningful insights to support services. The number of such IoT devices currently present in the world [33] are multiple times that of the world population. To enable these devices to exchange data,

wireless technologies need to be used as physical connections would, for one, be too costly (where ever they can be used), second, would not satisfy the mobility requirements that are typical of many smart city applications. The internet has provided connectivity to computers, smartphones and other electronic devices around the world with each other, allowing for instant transfer of information between them. However, for IoT the internet may not necessarily be the only communication method [67] as many applications do not possess edge devices that can connect to the internet. An application may consist of a local network of sensing units which can exchange data between them and rely on a multi-hop communication protocol to send data to a central node, hub or gateway. The gateway might be fixed and would be connected to the internet, thereby relaying any monitored data to the cloud for further processing or use. It might also be possible that devices within an application may use many different protocols with the central node having the capability to communicate with all of them, a common case for such architectures is the smart home where manufacturers produce devices using propriety or incompatible protocols for which a hub may be used, an example of such a system was provided in [68] and several hubs are commercially available. In this section, we discuss the network types, topologies and protocols used in the Internet of Things for Smart City applications as illustrated in Figure 6. We later provide a comparison of these protocols in Table 4.

3.4.1. Network Topologies

There are three IoT network topologies, point to point, star and mesh [69]. The first type of topology is the point to point topology where devices are connected to each other sequentially in a point to point manner. Point to point networks introduce data hops for packets that need to be sent to other nodes as data needs to go through each node in the path of the two nodes wanting to exchange data. Point to point networks are not very popular in IoT systems as it ranks low on fault resiliency and will breakdown if there is a fault in any of the intermediate nodes. In Star topology, all units in a network are connected to a central node or gateway and cannot send data to each other directly. In order to perform an exchange of data among themselves, the devices need to send it through the central node. Star topology networks, with their central node structure provide a natural aggregation scheme for data collection within the internet of things, however, large networks consisting of many devices, which can be the case in most smart city applications, may result in high latency and possible bottlenecks in high information throughput scenarios. Star topology has been used in various applications including disaster management [70] and environmental sensing [71]. The last type of network topology that is used in IoT is the Mesh network topology, mesh networks allow all individual devices to communicate between them. By enabling communication between the nodes in a network, mesh topology offers a larger range as data transmitted towards a certain node can make multiple hops through the network, this also increases the networks resilience as alternate paths could be used if packet delivery fails due to any node becoming faulty. In fact, such topologies have been used in smart homes [72] as well as in smart grids [73]. There are other topologies which have not been mentioned, for, e.g., tree (which has multiple star networks connected in a point by point fashion).

3.4.2. Network Architectures

Network Architecture refers to the structure of the network used for a given application. As discussed earlier, the 'things' in IoT may not necessarily be connected through the internet, in fact a distributed connectivity structure may be implemented with only one unit in the network being capable of sending data to the cloud depending on the requirement. Work in [67] mentions three types of network architectures that are used for smart cities based on IoT. These are Home Area Networks (HANs), Wide Area Networks (WANs) and Field/Neighborhood Area Networks (FANs/NANs). Home Area Networks are short range networks and are usually used to transmit information to a central node which is responsible for data collection before it is sent to the cloud. Communication

within the network is performed using some low power communication protocol such as Zigbee, Bluetooth, Wi-Fi etc. HANs are very popular in smart homes where they are used to gather power consumption and times of operation data from a multitude of appliances which are then sent to a smart meter as part of a smart grid [74]. The second type of network architecture is Field Area Networks (FANs), sometimes also called Neighborhood Area Networks (NANs). Field Area Networks have a larger communication range than HANs and are used to provide connection between a customer (for, e.g., in a smart grid) to the utility company. Wide Area Networks are used for network structures that require communication over large distances. These networks are not as dense as HANs or FANs and utilize technologies such as cellular services, wired connections such as fiber optics as well as a class of low power protocols designed for WANs themselves [75]. WANs are used in a variety of smart city applications including Smart Grids where they are used to connect multiple substations together or exchanging data between the customer and the substation [76].

3.4.3. Network Protocols

The type of network to use depends on the requirements of the application. It is imperative that the communication protocol used in a smart city application meet the desirable quality of service (QoS). Several protocols have been used in the internet of things for smart cities [11,77–79], we discuss the traits of the most popular wireless networking protocols used in smart cities.

RFID

Radio Frequency Identification (RFID) utilizes radio frequencies to transmit and receive data. RFID communication consists of two types of devices, one device is the Reader and the other is called the Tag. The Reader is usually powered and once a tag comes in the vicinity of the reader, an exchange of information takes place after authorization as the tag harvests the energy from the reader. Such tags are called passive tags, there are also active tags which do not depend on the reader for their power. Depending on the standard, RFID can operate on different frequencies in the radio frequency spectrum between 125 KHz to 928 MHz and can be used over short ranges. They are used in applications such as smart transport (toll tax collection, parking), smart health and more.

Near Field Communication

Near Field Communication (NFC) is very similar to RFID, however, the structure of NFC communication doesn't consist of tags and readers. Unlike RFID, both devices which want to communicate using NFC need to be powered and data transmission/reception can take place in both directions unlike RFIDs. This enables the use of NFC to control and configure devices unlike the RFID which cannot be used for measurement or control tasks. NFC utilizes similar frequencies to RFID but is used for very short distances. NFC devices are popular for applications involving payment using smart phones and are also used in smart homes.

Bluetooth

Bluetooth is a low energy protocol popular in IoT applications as it can support an unlimited number of nodes [77]. The protocol is designed for short range, low bandwidth communication in an arrangement where devices can easily exit or enter the network. Bluetooth natively supports the star topology as it has a master device at the center of the communication mechanism. It operates in the 2.4 GHz ISM band and can have maximum data rates of 2 Mbps. Bluetooth has been widely used in smart home due to it providing a direct connection interface to smart phones without the need for any intermediary hub device.

Z-Wave

Z-Wave or Zensys wave is a low power protocol developed to be used in home automation applications. It is a low speed protocol with a short range, operating in the frequencies of 868 MHz and 900 MHz. It operates in a master slave fashion where a master can have multiple slave devices which can respond to commands from the master node, therefore this is well suited for applications where a central control element is present and needs to gather data from multiple sensing units such as smart homes and smart healthcare systems.

Li-Fi

Li-Fi (Light Fidelity) uses visible light instead of radio frequency to exchange data. The advantage with using Li-Fi over RF communication is that it can utilize already present lighting systems which also results in conservation of power [80]. It offers very high speeds of data transfer for short distances and has been used in parking systems.

Wi-Fi

Wi-Fi (Wireless Fidelity) operates using wireless frequencies in the 2.4 GHz and 5 GHz bands to provide high speed internet connectivity in a limited distance. Wi-Fi is popular in many smart city applications as it provides ready to use interface to smart phones, computers and other wearable gadgets.

Zigbee

The ZigBee protocol was developed as a low power low cost protocol for wireless sensor networks (WSNs) and has evolved to be used in the Internet of Things. The ZigBee protocol operates in the 868 MHz/915 MHz/2.4 GHz band and offers moderate data transfer speeds with distances similar to Wi-Fi in a multi-hop data transfer scheme. Zigbee radios are low cost devices and therefore it is a popular protocol used by many manufacturers of smart home, smart healthcare devices. A ZigBee network will have three devices, one called the coordinator which is the controller of the network, the router which is responsible for moving data to other devices and the ZigBee end device (sensors and actuators).

Wi-SUN

The Wireless Smart Utility Network (Wi-SUN) is a network approved by IEEE and is used in field area networks for utility metering, automation of distribution for utilities such as electricity, gas etc. and also for demand response systems for utility-based applications. It supports IPv6 addressing and can be used in star or mesh configuration where it also allows for multi-hop communication [81].

Cellular

Cellular technologies refers to 3G, 4G and 5G communications. Along with Bluetooth and Zigbee, they are the most popular IoT enabling technologies. Cellular communication provides high data rate and supports more content rich applications compared to the other protocols. With the long range they provide, they are preferred for a variety of applications where power is not an issue. Depending on the technology, cellular bands range from 600 MHz to 80 GHz with very high data rates.

LoRaWAN

LoRaWAN stands for Long Range Wide Area Network (LoRaWAN) and it is a Low Power Wide Area Network (LPWAN) that consists of several gateways and multiple end devices with the gateways connected to a back-end network server. The back-end server provides connection to the cloud. End devices do not have a fixed association with a specific gateway and may send data to multiple gateways when it needs to transfer data to the cloud.

6LoWPAN

6LoWPAN which is short for IPv6 over Low Power Networks was created by the Internet Engineering Task Force (IETF) specifically for internet of things applications with the aim of making it possible for providing internet connectivity to small devices. It is an IP based network and leverages IPv6 communication. This is a short-range network operating in ISM bands.

SigFox

SigFox is a proprietary standard developed by SigFox Inc., France. It uses unlicensed bands to perform ultra-narrowband bidirectional communication with low speeds [82]. SigFox has a similar architecture to LoRaWAN and like LoRaWAN and 6LoWPAN, SigFox is a popular LPWAN in the IoT domain offering sufficiently large distances of communication of up to 50 km. SigFox finds applications in security in buildings, smart lighting and environmental monitoring.

NB-IoT

NB-IoT (Narrow Band IoT) is a type of LPWAN which operates on Global System for Mobile Communications (GSM) and Long-Term Evolution (LTE) bands. In fact, it can operate using the same hardware with a software upgrade as it is considered a bare bones version of LTE. It allows for connecting up to 100,000 devices per cell.

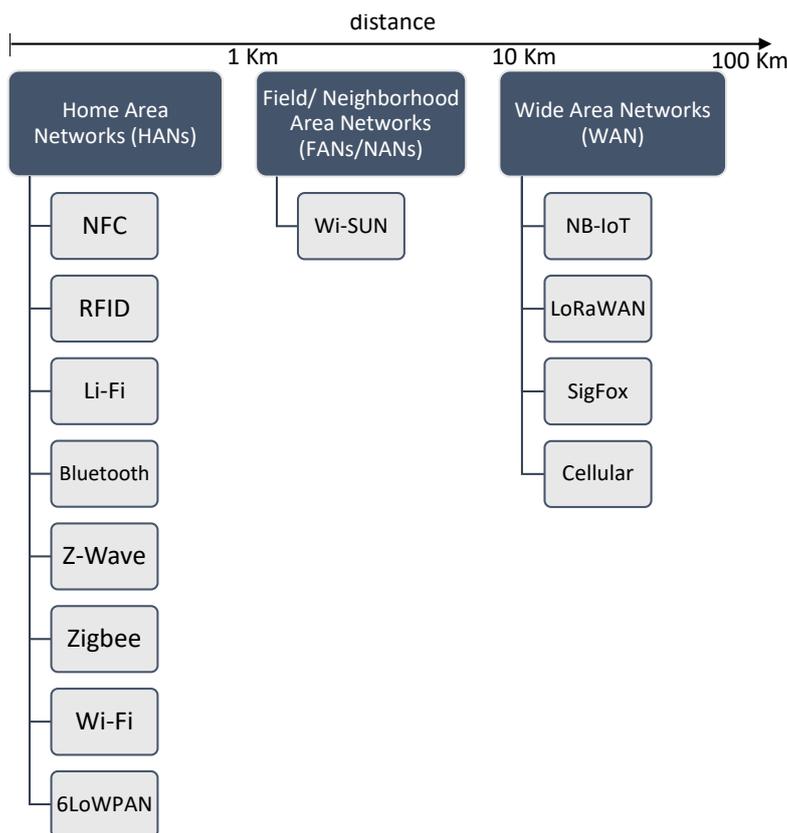


Figure 6. Network Technologies for IoT Smart Cities.

Table 4. Comparison of Network Technologies for IoT Smart Cities.

Architecture	Technology	Frequency/Medium	Data rate	Range	Topology
Home Area Networks (HANs)	NFC	125 KHz, 13.56 MHz/860 MHz	106 Kbps, 212 Kbps or 424 Kbps	10 cm	Point to Point
	RFID	125 KHz, 13.56 MHz/902–928 MHz	4 Mbps [77]	3–10 m	Point to Point
	Li-Fi	LED Light	1–3.5 Gbps [80]	10 m	Point to point, Star, Mesh
	Bluetooth	2.4 GHz	Up to 2 Mbps	240 m	Star
	Z-wave	868 MHz/900 MHz	40–100 Kbps	30–100 m	Mesh
	Zigbee	868 MHz/915 MHz/2.4 GHz	250 Kbps	Up to 100 m	Mesh, Star, Tree
	Wi-Fi	2.4 GHz/5 GHz	54 Mb/s, 6.75 Gb/s	140 m, 100 m	Tree
	6LOWPAN [77]	868 MHz/915 MHz/2.4 GHz	Up to 250 Kbps	10–100 m	Mesh, Star
Field/Neighborhood Area Networks (FANs/NANs) Wide Area Networks (WANs)	Wi-SUN	868 MHz/915 MHz/2.4 GHz	Up to 300 Kbps	Up to 4 km	Star, Mesh
	NB-IOT	Licensed LTE bands	200 Kbps	1–10 km	Tree
	LoRaWAN	433 MHz/868 MHz/915 MHz	Up to 50 Kbps	5–20 km	Star of Star (nested star)
	Sigfox	433 MHz/868 MHz/915 MHz	100 bps	10–50 km	One hop star
	3G	1.8–2.5 GHz	2 Mbps	-	Tree
	4G	600–5.925 GHz	up to 1 Gbps	-	Tree
	5G	600–80 GHz	Up to 20 Gbps	-	Tree

3.5. Big Data Algorithms/Artificial Intelligence

The various sensors that make up the internet of things in a smart city relay information about the city's state to the cloud. However, measuring raw data is not enough, to utilize this data and to make the city 'smart', data analysis is key. Data analysis in smart cities has four layers, the first is Data Acquisition, which deals with the collection and storage of data, this is followed by the Preprocessing layer which performs operations (such as imputing missing values, scaling, removing erroneous data points etc.) on the data to ensure that data is of suitable quality to be used for the data analytics stage. The data analytics stage involves the application of data science techniques on the data to extract patterns and insights which would be used for policy making, planning and other actions in the Service layer. In this section, we focus our attention on the third stage of the data analysis process, i.e., data analytics. Data analytics in the Smart City based on the IoT involves the use of Deep Learning and Machine Learning on the gathered data. Figure 7 provides a summary of the AI discussion in this paper. It highlights the applications in which each AI domain finds for smart city components. We first mention the algorithms most commonly used in smart cities and follow it up with a discussion for the application for each component.

3.5.1. Machine Learning

Machine learning (ML) has been a crucial element of smart city application development [83], helping in prediction (classification), estimation (regression) and clustering tasks. Machine learning refers to the set of approaches through which computers can be used to learn from empirical data [84] and has been used in smart cities in various applications. Since there has been a lot of work in this area using ML algorithms, we focus on work in the last five years. It was found that most commonly used ML algorithms have been the Support Vector Machine (SVM), Random Forests (RF), Decision Tree (DT), Naive Bayes (NB), K-Means, K-Nearest Neighbor (K-NN) and Logistic Regression (LR).

3.5.2. Deep Learning

Deep learning is the use of successive layers of Artificial Neural Networks (ANNs) to learn patterns. The idea is that successive non-linear layers of interconnected artificial neurons can be used to learn patterns in data that simple machine learning algorithms might not be able to do. Deep learning architectures can process noisy data to provide output for classification and prediction tasks. This makes them very useful in the Smart City environment where the IoT enables the collection of heterogeneous sensor data which can be of varying nature. Data derived from sensors can be processed to extract features or can be fed directly to deep learning algorithms which can perform both feature extraction as well as classification/prediction. Deep Learning methods such as Recurrent Neural Networks (RNN)(Long Short-Term Machines (LSTM) and Gated Recurrent Units (GRU)), Convolutional Neural Networks (CNN), Deep Neural Networks (DNN) and Stacked Autoencoder Networks (SAE) were the preferred deep learning methodologies used for smart city applications and our discussion revolves around the utilization of these methods.

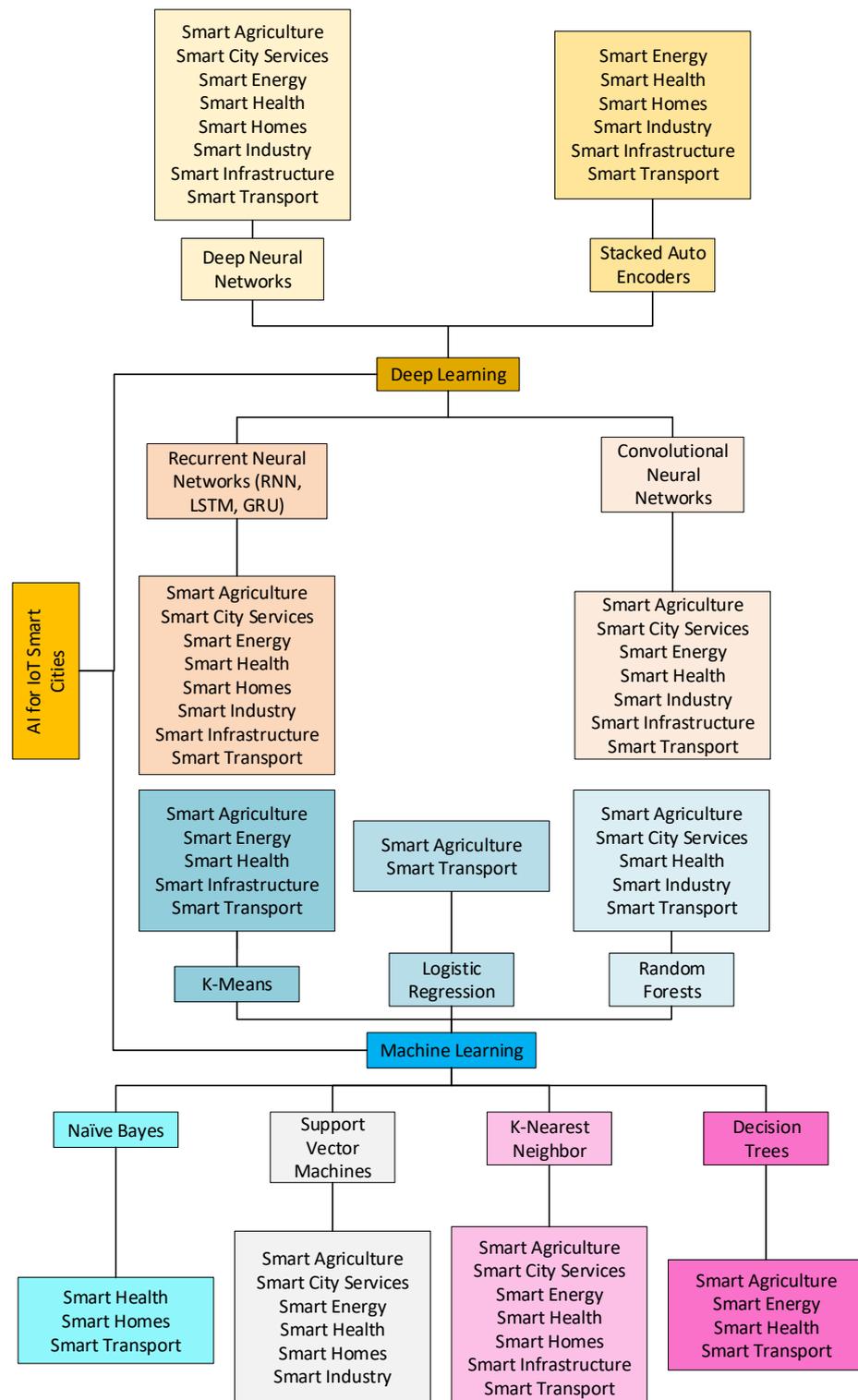


Figure 7. AI for IoT Smart Cities.

3.5.3. AI Use for Smart Cities

In this section, the applications for of AI in smart cities have been discussed, we also mention the kind of deployment as well as the nature of data utilized to achieve their task.

Smart Agriculture

The major applications of AI in IoT for agriculture are crop monitoring/disease detection and data driven crop care and decision making. Considering the scarcity of water, the authors in [85–87] develop irrigation systems which monitor and control the amount of water being used for crops, all structured around a cloud computing system. This problem has been devised both as a classification as well as a regression problem as in [88], who develop a closed loop water irrigation system using support vector regression and K-Means clustering. The authors in [89,90] propose cloud based greenhouse monitoring systems using images and a host of physical parameters from plants such as temperature, humidity and light using several machine and deep learning methods. Plant disease detection is also an important task within smart agriculture and has been worked on by the authors in [91–94] who present schemes for disease detection for various crops including tomatoes and potatoes. The proliferation of sensing systems in agricultural fields has also provided an avenue for data driven decision making and planning for farmers. This involves predicting various physical parameters which can affect crop growth like solar radiance [95] and temperature, humidity, windspeed [96–100] to help in decision making in terms of plant care but also classification systems for recommending crops to be sown [101,102]. It is important to note that all of these implementations are cloud based.

There have been some suggested methodologies for bringing fog processing for AI in smart agriculture, for, e.g., in [103] a deep learning entrusted to fog nodes (DLEFN) algorithm is described to support efficient use of resources and reduce cloud resource usage. However, as noted in [104], who use an edge system for temperature prediction using an LSTM, edge device performance still lacks that of similar cloud systems but the inclusion of DL capable hardware does provide opportunities for further innovations. Previous work by the same author [105], where they aimed to monitor crops for frost signs and trigger anti-frost measures, compared edge and cloud computing systems for outlier detection and determined that cloud implementations to provide much better performance. However, they do note the potential for edge systems to provide highly responsive data analytics in smart agriculture. More applications can be envisaged for AI deployment in smart agriculture, for, e.g., monitoring of crop growth, selection of the fertilizer and the timeline for it to be used as well as targeted application, pest detection and intelligent pesticide spraying so as to reduce harm to the environment, environmental monitoring to track the effects of climate change and more. Some of these applications have potential to be deployed as edge computing systems. A summary of the use of IoT based AI in Smart Agriculture is presented in Table 5.

Table 5. AI use for Smart Agriculture.

Application	Network	System Architecture	Task	Data Type
Crop Monitoring/Plant care (Irrigation)	LR [85]	Cloud	Classification—Different states of crop [less water etc.]	Heterogeneous (Temperature, Soil moisture, Air quality, Sunlight etc.)
	DT [87]		Classification—Different conditions of plants and soil [dry etc]	Homogeneous (Images)
	CNN [86]		Regression—Predicting amount of moisture in soil	Heterogeneous (Soil moisture, Soil temperature, Air temperature, Ultraviolet (UV) light radiation, Relative humidity, Weather forecast data)
	SVR + K-Means [88]			
Crop Monitoring/Plant care (Monitoring and disease detection)	SVM [89]	Cloud	Regression—Forecasting temperature	Heterogeneous (Temperature, Humidity, Light, Soil moisture)
	SVM [92]		Regression—Daily crop growth (indirectly from measured data)	
	SVM [91]		Classification—Different crop conditions	Heterogeneous (Images, Gas)
	SVM + K-Means + CNN [90]	Classification—Different stages of tomato growth	Homogeneous (Images)	
	SVM [93]		Classification—Recognizing and detecting disease	
	CNN [94]	Edge		

Table 5. Cont.

Application	Network	System Architecture	Task	Data Type
Data driven crop care and decision making (Predicting physical parameters)	CNN + RNN(GRU) [96]	Cloud	Regression—Prediction of Temperature, Humidity and Wind speed	Heterogeneous (Temperature, Humidity, Wind speed, Location of monitoring station, Time, Rainfall, Solar radiation)
	RF [100] RNN (LSTM) [97] DNN [99] RNN (GRU) [98]			
	DNN [95]		Regression—Prediction of solar radiance Regression—Temperature forecasting	
	RNN (LSTM) [104]	Edge /Cloud		
Data driven crop care and decision making (Crop recommendation)	DT [101]	Cloud	Classification—Different crops	Homogeneous (Temperature)
	DT [102]		Classification—Soil fertility and type, Regression—Prediction of soil toxicity	Heterogeneous (Soil moisture, Temperature, Humidity, PH, Soil nutrient content/fertility)

Smart City Services

A popular component of smart city initiatives is the management of waste and involves having bins equipped with sensors and connected to the cloud to not only inform the relevant authorities of the need to empty them but also using AI to determine the best route to reduce fuel consumption. The use of IoT systems for waste management has been observed in the works of [106] who utilize IoT systems to help reduce energy wastage in waste collection by municipalities. Hussain et al. [107] develop a waste management system that not only determines if bins are full and need collecting (using data from various sensors placed in the bin) but also predicts the air quality around it using RNNs. The sensing modalities in each of these applications is pretty similar in that they indicate to whether a waste bin is full or not which is then used for route planning. Considering the requirements of such a system, in terms of implementation, all of these systems are cloud based. Sewer monitoring has been performed in [108] in a cloud based system, they use sewer water level and rain gauge data along with a RNN to perform sewer overflow monitoring. The RNN is used to predict sewer overflow ahead in time. Water quality has monitoring has been the focus of [109–111] where the authors use multiple sensors measuring pH value, chloride, nitrate content and hardness of water to determine whether it is fit for drinking or not. In [112], Liu et al. use data from water monitoring stations along the Yangtze river to predict water quality. Like the classification-based systems, they use multiple chemical measurements from the water such as oxygen, pH, turbidity etc. Apart from air quality, smart city monitoring systems are an important application within the smart city services domain. This includes urban noise, which has been the focus of researchers in [113,114] as well as other more comprehensive monitoring systems as proposed in [115,116]. All these systems are cloud based and use a combination of sensors for sound and/or image data for performing noise monitoring/detection and various smart city dashboard applications. In Table 6, we summarize the type of deployments, applications task and data for smart city services applications. It is noted that most of the applications relating to city services such as air quality monitoring and prediction, sewer monitoring, waste collection have been proposed as cloud systems as data needs to be collected from nodes at various points in a city. It is envisaged that due to the nature of the applications, many smart city services would still rely on cloud or fog architectures as the decision-making taking place in such situations isn't possible on only a local level. It is also observed that most of the applications required data from multiple sensors and therefore utilized heterogeneous data to carry out the task at hand.

Table 6. AI use for Smart city Services.

Application	Network	System Architecture	Task	Data Type
Air quality	K-NN [117]	Cloud	Classification—Differentiate between different air quality levels	Heterogeneous (Gas, Light, Temperature, Humidity, Pressure, Wind speed, Weather information, Images, Traffic flow data, Visibility, information about types of buildings etc.)
Water quality monitoring	RF [118] RF [119] RNN (LSTM) [120]	Cloud	Regression—Prediction of air quality levels	Heterogeneous (Chlorides, Nitrates, Total dissolved solids, pH and Hardness, and other chemical properties)
	NB [109]		Classification—Determine if water is fit to drink or not	
Sewer Overflow Monitoring	SVM [110] DNN [111] RNN (LSTM) [112]	Cloud	Regression—Prediction of water quality	Heterogeneous (Water level sensor data (ultrasonic) over drain holes as well as rain gauges)
	RNN (GRU, LSTM) [108]		Regression—Prediction of when	
Waste management	RNN (LSTM) for prediction of air quality [107], K-NN for detection of waste bin being full RF [106]	Cloud	Regression—Prediction of air pollutant levels, Classification—Bin full or not Classification—Empty bin or not	Heterogeneous (Odor, Weight, Level sensing using ultrasonic sensor, Gas sensor for air quality, Vibration)
Urban noise monitoring	CNN [113]	Cloud	Classification—Different types of sounds	Homogeneous (Sound)
	RNN (LSTM) [114]		Regression—Prediction of noise levels	
Management of Smart City	CNN [116]	Cloud	Application—Dashboard (object identification etc.)	Heterogeneous (Various sensors, Urban video and sound data)
	CNN [115]			

Smart Energy

Load/energy consumption forecasting is an essential task for monitoring and control of electrical power supply in the electricity grid and ensure appropriate demand side management. It has been performed by the authors of [121] who use data collected from consumers in a smart grid to determine load for up to 24 h in advance. They treat this as primarily a clustering problem where they form clusters of similar load profiles and then use distance functions to determine energy consumption for the future. The authors in [122] also use a cloud based clustering approach, using historical power data, they use K-Means clustering to determine the closest historical records and then combine them to predict energy consumption 24 h in advance. The load forecasting problem has been dealt as a regression by [123] using a SVM and by [124] through an RNN using electricity power data. A regression approach is also followed by [125,126] who use electricity consumption in addition to environmental data for load forecasting using deep learning methods (DNN and a combination of Autoencoders and RNNs (GRU)). Edge based systems have been suggested by the authors of [127–129] for load forecasting for household consumers, Ref [129] use federated learning to train a RNN. In addition to load forecasting, smart grid management/monitoring is also a necessary application in this domain. The authors in [130] use decision trees in a cloud based system to classify between different faults in a smart grid. In [131], the authors use power consumption data from consumers in China to determine electricity theft in a cloud based system. They use wide and deep convolutional neural networks to capture the periodic and nonperiodic components from electricity consumption data and show their network to be suitable for electricity theft detection. The authors in [132] present a framework for edge computing based monitoring of the smart grid. Edge computing in the smart grid has several advantages as it reduces delay and secure in terms of data privacy. A summary of the use of IoT based AI in Smart Energy is provided in Table 7.

Table 7. AI use for Smart Energy.

Application	Network	System Architecture	Task	Data Type
Energy/Load consumption forecasting	K-Means [121]	Cloud	Clustering—Determine clusters of similar power consumption Regression—Predict consumption of electricity ahead of time	Homogeneous (Electric power)
	K-NN [122]			
	SVM [123]			
	RNN (LSTM) [124]			
	DNN [125]			
Smart Grid line event classification (fault etc.)	SAE + RNN (GRU) [126]	Edge		Heterogeneous (Electric power, Temperature, Humidity, Time, Holiday)
	CNN [128]			
	RNN (GRU) [127]			
	RNN (LSTM) [129]			
Electricity theft detection	DT [130]	Cloud	Classification—Different powerline events	Homogeneous (Electric power)
	CNN [131]	Cloud	Classification—Theft detection for abnormal patterns of consumption	Homogeneous (Electric power)

Smart Health

There are two major applications of IoT with AI in health, these are activity recognition/fall detection and disease diagnosis/health monitoring, a summary of the IoT based AI systems used in Smart Health is presented in Table 8. Activity recognition involves the use of movement sensors such as accelerometers, gyroscopes and magnetometers with the aim to help provide the user with feedback on their health in terms of them having enough physical exercise or not, used for sports therapy, fall detection and for monitoring of different diseases such as Parkinson's or other motor degenerative ailments. The most popular sensor for activity recognition are inertial sensors which have been used by [133,134] in a cloud based setting using various deep and machine learning algorithms. In [135], Castro et al. include vital sign data in addition to movement information for human activity recognition in a cloud environment, they utilize the DT as their classifier. In [136], the authors propose an edge-based system to perform activity recognition for people by recording their movements using the accelerometer and gyroscope present on the phone. They use a SVM as their classifier and differentiate between six different activities of daily living. Fall detection has been performed by [137,138] in a fog and edge environment, respectively, using an accelerometer, Santos et al. [137] use a CNN while Yacchirema et al. [138] use RF with both approaches showing promising results.

Equipped with the power of AI in IoT, Smart Health systems facilitate the provision of telehealth services as well as real time monitoring of patients, giving doctors and patients feedback on their health. Health monitoring systems and real time disease diagnosis have been one of the most important applications of IoT technology. The authors in [139–149] develop cloud based health monitoring systems for detecting various types of diseases, such as heart (stroke [140], irregular sound [142], irregular rhythm [144,146]), epileptic seizures [145], Parkinson seizure [149] and multiple disease diagnosis systems [147,148]. In [147,148], the authors formulate the problem of disease diagnosis as a classification problem and utilize medical data such as ECGs, EEG, heart rate, blood pressure, blood sugar, heart sound, blood glucose, liver health along with various machine and deep learning methods to achieve this task. Fog and edge based health monitoring/disease diagnosis systems have also been suggested by a number of researchers. The authors in [150] present a fog based system using a deep neural network to detect heart disease from a patients vital signs (blood oxygen, heart rate, respiration rate, EEG, ECG, EMG, blood pressure, glucose) and activity data. In [151], Devarajan & Ravi work on a fog computing based Parkinson detection system using a persons speech. Moreover, an edge computing system is presented in [152] which utilizes EEG signals to determine seizures in patients.

Table 8. AI use for Smart Health.

Application	Network	System Architecture	Task	Data Type		
Human activity recognition/Fall detection	DT [135]	Cloud	Classification—Different activities, fall/non falls	Heterogeneous (Acceleration, Heart rate, Posture, ECG, Respiration rate)		
	RF [133]	Fog Edge		Homogeneous (Accelerometer)		
	CNN [134]			Heterogeneous (Accelerometer, Gyroscope, Magnetometer)		
	RNN (LSTM) [153]			Heterogeneous (Accelerometer and Gyroscope)		
Patient health monitoring	CNN [137]	Fog	Classification—Recommendation about diet etc.	Heterogeneous (Heart rate, Sleep, Calories burned, Weight, Physical activity time, Water, Exercise etc.)		
	RF [138]	Edge		Heterogeneous (Speech and Image)		
	SVM [136]	Cloud		Heterogeneous (ECG, BVP, GSR, SKT, EMG)		
	DT [139]			Homogeneous (EEG)		
	SVM [142]			Classification—Different emotions		
	Disease diagnosis	RNN(LSTM) [154]		Cloud	Classification—Abnormal/normal heart sounds	Homogeneous (EEG)
		CNN + SAE [145]			Classification—Epileptic Seizure detection	Homogeneous (Heart sounds)
RF [141]		Classification—ECG arrhythmias	Homogeneous (ECG)			
SVM [144]		Classification—Different heart diseases	Heterogeneous (Heart health information, Patient records and other health sensors)			
DT [146]		Classification—Kidney, Heart and Liver disease	Heterogeneous (Heart and Kidney health data)			
K-Means [147]		Classification—Detection of various diseases	Heterogeneous (Diabetes, Heart, Liver, Dermatology etc data)			
Parkinson detection	RF [148]	Fog	Classification—Presence of heart disease or not	Heterogeneous (Blood oxygen, Heart rate, Respiration rate, EEG, ECG, EMG, Blood Pressure, Glucose and Activity data)		
	DNN [150]		Classification—Parkinson detection/stroke has happened/seizure detection	Heterogeneous (Blood pressure, Sugar, Pulse rate)		
	RF [140]		Cloud	Classification—Parkinson detection/stroke has happened/seizure detection	Heterogeneous (Blood pressure, Sugar, Pulse rate)	
Seizure monitoring	SVM [149]	Fog		Homogeneous (Speech)		
	K-NN [151]			Edge	Homogeneous (EEG)	
	NB [152]			Edge	Homogeneous (EEG)	

Smart Homes

Ambient assisted living is a huge component of Smart Homes. This is especially needed for the elderly and is typically achieved by the use of ambient sensors, Wi-Fi and radio frequency systems in smart homes. In this work, we include all monitoring methods that depend on sensors placed in the home/within the smart home domain. In [155], Pirzada et. al use a network of reed switches connected to the cloud to monitor the activities of elderly people as a clustering problem. They use the K-NN algorithm to determine anomalies in the daily activities which can then be used to send medical or other help requests to assist people. A similar setup for activity recognition for ambient assisted living has been presented in [156–158] where they use data from a number of different sensors including motion, presence, water float, temperature etc to determine various activities being performed in a home. In [159], a cloud based assisted living system for the deaf has been developed that performs haptic conversions for sounds detected in a home. An array of sensors are used to monitor environmental sound and the authors use RNNs for detecting the sound event before its passed on to the haptic vibration producer. Another task within in monitoring is localization of people, this part of smart homes is also applicable to smart infrastructure in that such systems are used in smart buildings as well. Applications of localization include security, i.e., detecting unauthorized presence and people monitoring in general (for, e.g., locating elderly people in homes) etc. The authors in [160] perform localization using a grid of Wi-Fi units that measure signal strength to determine peoples locations indoors for buildings. They formulate this both as a classification problem as well as a regression problem. The classification problem being formulated as coded locations (for, e.g., a given room no) while the regression case estimating the location of the user in a coordinate grid. Their system is cloud based and they use a deep neural network to perform this task and have found suitably good results. Occupancy detection has been performed by the authors of [161] making use of various ambient measurements (temperature, humidity, pressure etc.) and passing them to a cloud before using a deep neural network to classify between the various number of people

present in an indoor environment. In [162], Zimmermann et al. also make use of ambient sensors for the occupancy problem and use a naïve bayes learner to determine both the presence of occupants as well as their number. Home automation is another application that the IoT finds application within the Smart Home domain. The integration of AI has helped develop smart home automation systems that aim to reduce energy consumption in homes as well as maintain user privacy, security. Chowdhry et al. [163] use a combination of visual data and motion sensing to perform home automation for security using a SVM. An interesting use of AI in home automation is presented in [164] who develop a cloud based home automation system, they take measurements from various ambient sensors and control appliances and use a Naïve Bayes classifier to determine which technician to call whenever sensor measurements appear aberrated. The problem of Intelligent consumption of energy has been considered by [165] who develop an energy disaggregation system on the appliance level in smart homes using stacked denoising autoencoders. They achieve this using power data for individual appliances as well as the total power consumed in the home and send it to a local cloud. Data are then disaggregated for various appliances to provide feedback to the user. More work providing energy intelligence to consumers has been performed by [166–168]. Konstantakopoulos et al. [168] pose this as a regression problem, they propose a cloud-based system utilizing both ambient sensor data (lighting, temperature etc) and appliance power data to forecast resource usage for consumers using a RNN. They show a reduction in energy consumption for their users using this information.

Eventhough applications covered in smart homes have been cloud based systems, there have been recent proposals for frameworks that combine edge and cloud processing as in [169] who discuss a hierarchical control system for smart homes through a edge microgrid and a cloud power grid. Due to the nature of smart homes in that the sensing scheme is present within a finite space (within the home), edge and fog computing based systems are expected to be increasingly incorporated smart home applications. A summary of the use of IoT based AI in Smart Homes is presented in Table 9.

Table 9. AI use for Smart Homes.

Application	Network	System Architecture	Task	Data Type
Ambient Assisted living (Activity recognition/Fall detection)	EFEFEFK-NN [155]	Cloud	Clustering—Detect abnormal clusters	Homogeneous (Reed switches)
	RNN (LSTM) [158]		Classification—Different activities	Heterogeneous (Human motion, Water float, Reed switches, Temperature, Pressure, Luminance, Gas and other environmental sensors in a home)
	RNN (LSTM) [156] SAE [157] RNN (GRU) [159]		Classification—Different sounds	Homogeneous (Sound recordings from rooms in a house)
Ambient Assisted living (Localization and Occupancy detection)	DNN [160]	Cloud	Classification and Regression—Localization estimation	Homogeneous (Wi-Fi signal strength and identifiers)
	NB [162]		Classification—Presence of people or not, Regression—Number of occupants	Heterogeneous (Volatile organic compounds, CO, Temperature, Humidity)
	DNN [161]		Classification—Different number of people present	Heterogeneous (Temperature, Luminance, Humidity, Pressure, CO ₂ , Motion, Magnetometer, Gyroscope, Accelerometer, Sound, Door and window open/close status)
Energy management (Automation, Power consumption profiling)	SVM [163]	Cloud	Classification—Intrusion detection	Heterogeneous (Images + Sound)
	SAE [165]		Regression—Disaggregation of appliance power data	Homogeneous (Appliance power consumption)
	RNN (LSTM)[168]		Regression—Forecasting occupant resource usage	Heterogeneous (Appliance power consumption, Luminance, Vibration, Temperature, Humidity, Accelerometer [fan])
	SAE for disaggregation and RNN(LSTM) for forecasting [167] NB [166]		Classification—Energy disaggregation, Regression—Load forecasting	Heterogeneous (Temperature, Luminance, Humidity, Proximity switches, Ultraviolet light sensors, Power consumption)
			Classification—Determine appliances that are on	Homogeneous (Appliance power consumption)

Smart Industry

One of the major applications of AI in the IoT powered smart industry is towards fault detection in products and anomaly detection in industrial processes. This has seen the use of both Machine Learning (SVM [170,171], RF [172,173] as well as Deep Learning (DNN [174–176], CNN [177]) methods using a cloud computing structure to perform anomaly detection /product inspection and monitoring using a variety of heterogeneous and homogenous data sources such as inertial sensors for machines, images for products and processes and other process specific variables. Other approaches suggested in [178,179] propose a fog computing method along with edge computing systems suggested in [180,181]. An edge computing system for anomaly detection is presented in [182] where edge devices collaboratively train a deep anomaly detection model. Production management is another application that has found usage of AI in IoT based smart Industry. For, e.g., the authors in [183–187] use cloud based data driven systems along with machine and deep learning algorithms to help with task dispatching, performance analysis as well as worker activity recognition utilizing a variety of sensing modalities. The work of [186,187] are especially interesting as they aim is to not only perform production management but also propose data for various health related analysis to create a safer working environment on the factory floor. A fog system for production management has been presented in [188] who use activity data to determine resource allocation locations to contribute to management of a production operation. Furthermore, product inspection, which is a common application of instrumentation systems in a factory, has been performed by [189,190] who utilize images and sensor data in a cloud based system to monitor product quality.

A factory has a multitude of machines and equipment working round the clock manufacturing goods. Maintenance is an important aspect of this operation where regular checks are performed on the equipment to ensure that no breakdown occurs during the production process, which might result in monetary loss or loss of life. However, with the data gathered by various sensors on these machines, it is often more beneficial to take an active approach rather than a passive one by using this data for predictive maintenance purposes. Predictive maintenance utilizes data from the daily operation of machines in an industry to optimize the manufacturing operation [191] and is one of the main uses for AI in the industry. In [192,193], the authors suggest a predictive maintenance scheme using SVMs utilizing data from accelerometers measuring vibration in a crane motor and data from various sources in a semiconductor manufacturing process, respectively, both work in a cloud environment as evidenced from the architecture. Prediction of failure can also be a regression operation, as was demonstrated by [194] who use RNNs to predict future values of a physical parameters of a pump using a number of heterogeneous sensors used to monitor it. As with the other two systems, this system also had a cloud architecture. The authors in [143] also present a regression based health prognosis system for the industry using a CNN on machine data (Images, stress, temperature, vibration, position and electromagnetic signal measurements). The use of IoT based AI in Smart Industry has been presented in Table 10.

Table 10. AI use for Smart Industry.

Application	Network	System Architecture	Task	Data Type
Fault and anomaly detection	DNN [176]	Cloud	Classification—Different classes of abnormality labels	Heterogeneous (Multiple sensor and controls [button states etc.] information)
	DNN [175]		Classification—Different damage stages of a 3D printer	Heterogeneous (Accelerometer, Gyroscope)
	RF [172]		Classification—Normal and abnormal operation in wind turbines	Homogeneous (Accelerometer)
	SVM [170]		Classification—Different wind turbine health conditions	
	SVM [171]		Classification—Normal and mixed cement	Homogeneous (Images)
	RF [173]		Classification—Different fault types in steel manufacturing	Heterogeneous (Various sensors, dimensional measurements)

Table 10. Cont.

Application	Network	System Architecture	Task	Data Type
Production management	DNN [174]	Fog	Classification—Normal and arcing	Homogeneous (Current)
	CNN [177]		Classification—Defected product or not	Homogeneous (Images)
	CNN [178]		Classification—Different types of defects	Homogeneous (Images)
	CNN [179]	Edge	Classification—Abnormal and normal pressure	Homogeneous (Water pressure)
	SVM [180]		Classification—Abnormal and normal time power patterns	Homogeneous (Electrical power)
	CNN + RNN (LSTM) [182]	Cloud	Classification—Faulty and normal state of a machine	Homogeneous (Accelerometer)
	RNN (LSTM) [181]		Regression—Prediction of the slotted coefficient in a hydraulic press	Heterogeneous (Various measurements from a hydraulic press)
	SVM [183]		Regression—Forecasting machine speed to make production more efficient	Homogeneous (Speed of machine [rotary])
	ConvLSTM + SAE [184]		Regression—Bottle neck prediction in time	Heterogeneous (RFID, movement sensors)
	DNN [187]		Classification—Different activities in an assembling factory	Heterogeneous (IMU, EMG)
CNN [185]	Classification—Different activities in a meat processing plant evaluate worker performance		Heterogeneous (Accelerometer, Gyroscope)	
SVM [186]	Classification—Bad or good product quality		Heterogeneous (Various sensors from a production floor in a factory)	
Predictive maintenance	RF [190]	Fog	Classification—Prediction of temperature, Carbon content in steel	Homogeneous (Spectrogram Images)
	CNN [189]		Classification—Determine Room ID, used for system disruption	Heterogeneous (Activity data, Location)
	RF [188]		Regression—Predict health index for machines	Heterogeneous (Images, Temperature, Vibration, Position, Electromagnetic signal measurements, Strain gauge)
	CNN [143]	Cloud	Classification—Abnormal or normal vibration data (from electric motor in a crane)	Homogeneous (Accelerometer)
	SVM [192]		Classification—Failure prediction	Heterogeneous (Multiple sensors from SECOM dataset)
	RF + SVM [193]		Regression—Predicting data from sensors	Heterogeneous (Different sensors [Pressure, Temperature, Vibration etc.])
	RNN (LSTM) [194]			

Smart Infrastructure

An application within smart infrastructures also involves monitoring of civil structures for structural health. The authors in [195] take a clustering approach to perform health monitoring of a bridge using vibration data in a cloud setting. They use clustering to determine clusters of abnormal behavior in accelerometer measurements from a bridge. In [196–198], accelerometer signals have been used where as [199] have used piezo electric transducers for performing structural health monitoring of bridges formulated as a classification problem between different damaged states of a bridge. The prime sensing modality for monitoring has been measuring vibration using accelerometers, however, other sensors such as fiber optic gratings can also be used to measure stress.

The second avenue for AI applications in IoT for smart infrastructure is the use of IoT devices for building environment control and energy management as well comfort aware control. This involves the prediction of building energy usage based on environmental data (such as temperature, humidity) and electrical power data. The authors in [200] and [201] use electric power data and heat flow information in a building to predict the energy requirements in the future so as to better manage energy consumption. Ambience control of a museum has been performed in [202] where the authors use deep learning algorithms to predict the CO₂ and humidity levels for the care of exhibits. Comfort aware energy management has been performed in [203] where the authors use a CNN to regulate thermal comfort in a building using various physical quantities. It can be noted that all of these mentioned systems have been deployed in the cloud, this is due to the nature of the application. However, there have been efforts for developing fog/edge systems for smart infrastructure. The authors in [204] describe a framework for deploying edge and fog computing services in smart buildings and demonstrate their systems effectiveness

for the case of energy management. Table 11 summarizes the use of IoT based AI in Smart Infrastructure.

Table 11. AI use for Smart Infrastructure.

Application	Network	System Architecture	Task	Data Type
Structural health monitoring	K-Means [195]	Cloud	Clustering—Look for abnormality of building state	Homogeneous (Accelerometers)
	K-NN [199]		Classification—Different damage states	Homogeneous (Piezo electric sensors)
	DNN [196]			Homogeneous (Accelerometer)
	CNN + RNN (LSTM) [198] SVM [197]			
Energy and Environment management	SVM [200]	Cloud	Regression—Forecasting electrical power usage	Heterogeneous (Power and environmental data)
	SAE [201]		Regression—Energy predictions for buildings	Homogeneous (Heat flow data in buildings)
	RNN (GRU, LSTM) [202]		Regression—Prediction of environmental variables (CO ₂ , Humidity etc.)	Heterogeneous (environmental data such as CO ₂ , Humidity, Air velocity)
	CNN [203]		Regression—Comfort level	

Smart Transport

Major smart transportation applications involve smart parking and transportation management. Smart parking aims to solve the problem of helping users finding parking spots in order to save time as well as reduce gas emissions and is therefore a much-researched topic for AI deployment towards smart transportation. Solutions to this problem have been formulated both as a regression problem as well as a classification one, both utilizing imaging and/or other occupancy sensing modalities. Regression solutions [205–207] are typically used to predict a parking lots occupancy levels in the future whereas classification systems [208–210] involve guiding drivers according to the shortest distance as well as used for user localization purposes within such lots. In addition to cloud based approaches, edge computing systems for smart parking have also been devised as suggested in [211,212] who deploy CNNs on edge devices for occupancy detection and user localization, respectively. Another application of AI IoT for smart transportation involves determining traffic flow as well as prediction of traffic flow for traffic light control and other management tasks such as accident detection. In this regard, video cameras are popular for detection of vehicle density on roads for traffic congestion determination. However, with most cars having a GPS device and the commonality of cellphones with every driver, many approaches use the data from the GPS along with weather and generic traffic flow information to determine traffic prediction. The nature of traffic flow prediction using sensing modalities such as GPS require systems to be operated as cloud-based systems as is the case in [213–216]. Of these, Wangyang et al. [215] and Xiao et al. [216] use deep learning based sequential modeling approaches to predict traffic flow ahead of time where as Aung & Naing [213] and Yunxiang Liu & Wu [214] solve this through a classification formulation. A traffic management system for public buses has been proposed in [32,217] where GPS data is used to predict bus arrival times for public transportation systems. Accident detection has been performed using car position and velocity information in a VANET environment by the authors of [218] in a cloud based system that can use this information to predict whether an accident has occurred or not. Apart from typical sensing modalities, with smart phones and user participation in social media, smart transportation systems are expected to increasingly include more sensing modalities [219] fused together for use in decision making for traffic management purposes. Mukherji et al. [220] use Wi-Fi signals to determine commuter traffic a subway station. They do this by using the measured signal strength of the Wi-Fi signals along with a Random Forest classifier in a cloud-based setting. Their system is able to determine if a person is on the train or on the platform which can be used to help with planning train times and routes. A summary of IoT based AI for Smart Transport has been given in Table 12.

Table 12. AI use for Smart Transport.

Application	Network	System Architecture	Task	Data Type
Smart Parking (Parking occupancy detection/Routing/Location prediction)	K-NN [210]	Cloud	Classification—Presence of a vehicle	Homogeneous (Images)
	K-Means [205]		Regression—Future occupancy prediction	Heterogeneous (Occupancy, Location, Time)
	RNN (LSTM) [207] LR [206]	Edge		Homogeneous (RFID data from cars)
	DNN+ CNN [208]		Classification—Different positions based on beacons installed	Homogeneous (Radio frequency signal strength)
	DT [209]		Classification—Recommendation of parking lot based on distance	Heterogeneous (Parking information, Time)
	CNN [211]		Classification—Detection of empty parking space	Heterogeneous (LIDAR, Images)
	CNN [212]		Classification—Different user locations localization	Homogeneous (Bluetooth received signal strength)
Transport management (Public transport management)	K-Means [32]	Cloud	Regression—Transport delay prediction	Heterogeneous (GPS, Ticket information, Time, Arrival, Departure information etc.)
	K-Means [217] RF [220]		Regression—Arrival time prediction Classification—Localization, as on platform or train	Homogeneous (Wi-Fi signal parameters)
Transport management (Traffic flow)	NB [213]	Cloud	Classification—Different traffic states	Homogeneous (GPS data, current and historical)
	RF [214]			Heterogeneous (Weather, Road data)
	RNN (LSTM) [216]		Regression—Traffic flow prediction	Homogeneous (Traffic flow data [vehicle speed count etc.]
	RNN (LSTM) [221] SAE + RNN (LSTM) [215] RF [218]		Classification—Accident or not	Homogeneous (Velocity, Position)
Transport management (Traffic Accident detection)				

Artificial Intelligence is the prime enabler of Smart City service provision as it facilitates the use of the data collected in a smart city. A summary of the discussion about AI use in IoT for Smart Cities in this section as well as the observations made are summarized in Table 13.

3.6. Security and Privacy in Smart City IoT

Smart Cities involve the transmission of sensing data, control information through the internet as well as local networks. Moreover, several components in smart cities tend to critical aspects of a city's operation and are being highly intertwined with the social and private life of its citizens. Consequently, security and privacy in Smart Cities is of great importance and has been of high interest to researchers [46,222–226]. The topic of Security of IoT has been covered in [227] who deliberate upon the challenges faced in the different architectures of the IoT and present issues and solutions. We cover security for IoT in smart cities so as to highlight issues that are pertinent to in the Smart City context and to complete our discussion on this topic.

Smart Cities are enabled by collecting data through sensors within a city as well as its populace, process it and then mine it to provide a better quality of life to the people living. These sensors can provide an estimate about the internal state of a city's components such as transportation, power system, building condition/state, human mobility and more. All these data are sent to the cloud where it is processed and mined. However, there are several issues that pertain to how these data are sent and used and raises questions about integrity, protection and the confidentiality of this process. In fact, this concern is not unwarranted for, in 2015 an attack on the Ukrainian power grid which left 225,000 people without power [228] opened the world's eyes to the very real threat posed by cyber attackers. Data gathered in Smart City applications can be used to perform many undesired acts, GPS devices that are present in every phone and most vehicles are susceptible to providing information about a person's location, habits as well as lead to privacy issues as discussed in [225], power consumption and ambient sensor data from a building may indicate to

occupancy [229] and even indicate to the individual identities [230]. This information may be used by bad actors to carry out unlawful acts causing risk to life and property.

To secure the Internet of Things for Smart Cities, typical security schemes might not be as effective in many cases and new methods will need to be developed to cope with the security and privacy issues in IoT for Smart Cities. In order to provide a standardized framework and terminology for discussing security attacks, we adapt the standard attack incident taxonomy [231] suggested by the Computer Emergency Response Team (CERT) which was established by DARPA for use towards IoT for Smart Cities. This is shown in Figure 8.

Table 13. AI applications for IoT Smart Cities.

Smart City Component	Machine Learning	Deep Learning	Observations
Smart Agriculture	<ul style="list-style-type: none"> - Crop Monitoring/Plant care (Irrigation) - Crop Monitoring /Plant care (Monitoring and disease detection) - Data driven crop care and decision making (Predicting physical parameters) - Data driven crop care and decision making (Crop recommendation) 	<ul style="list-style-type: none"> - Crop Monitoring/Plant care (Irrigation) - Crop Monitoring/Plant care (Monitoring and disease detection) - Data driven crop care and decision making (Predicting physical parameters) 	For applications such as Smart Agriculture, Smart Energy, Smart Health, Smart Industry and Smart Transport, Deep Learning as well as Machine Learning algorithms have been deployed in Edge/Fog configurations.
Smart City Services	<ul style="list-style-type: none"> - Air quality - Water quality monitoring - Waste management 	<ul style="list-style-type: none"> - Air quality - Water quality monitoring - Waste management - Sewer Overflow Monitoring - Urban noise monitoring 	
Smart Energy	<ul style="list-style-type: none"> - Energy/Load consumption forecasting - Smart Grid line event classification 	<ul style="list-style-type: none"> - Energy/Load consumption forecasting - Electricity theft detection 	The most popular machine learning algorithms were the SVM and RF.
Smart Health	<ul style="list-style-type: none"> - Human activity recognition/Fall detection - Patient Health Monitoring - Disease diagnosis - Parkinson detection/Seizure monitoring 	<ul style="list-style-type: none"> - Human activity recognition/Fall detection - Patient Health Monitoring - Disease diagnosis - Parkinson detection/Seizure monitoring 	
Smart Homes	<ul style="list-style-type: none"> - Ambient Assisted living (Activity recognition/Fall detection) - Ambient Assisted living (Localization and Occupancy detection) - Energy management (Automation, Power consumption profiling) 	<ul style="list-style-type: none"> - Ambient Assisted living (Activity recognition/Fall detection) - Ambient Assisted living (Localization and Occupancy detection) - Energy management (Automation, Power consumption profiling) 	
Smart Industry	<ul style="list-style-type: none"> - Fault and anomaly detection - Production management 	<ul style="list-style-type: none"> - Fault and anomaly detection - Production management 	
Smart Infrastructure	<ul style="list-style-type: none"> - Structural health monitoring - Energy and Environment management 	<ul style="list-style-type: none"> - Structural health monitoring - Energy and Environment management 	The most popular Deep Learning algorithms were RNNs and CNNs.
Smart Transport	<ul style="list-style-type: none"> - Smart Parking (Parking occupancy detection/Routing/Location prediction) - Transport management (Public transport management) 	<ul style="list-style-type: none"> - Smart Parking (Parking occupancy detection/Routing/Location prediction) - Transport management (Traffic flow) 	
	<ul style="list-style-type: none"> - Transport management (Traffic flow) - Transport management (Traffic Accident detection) 		

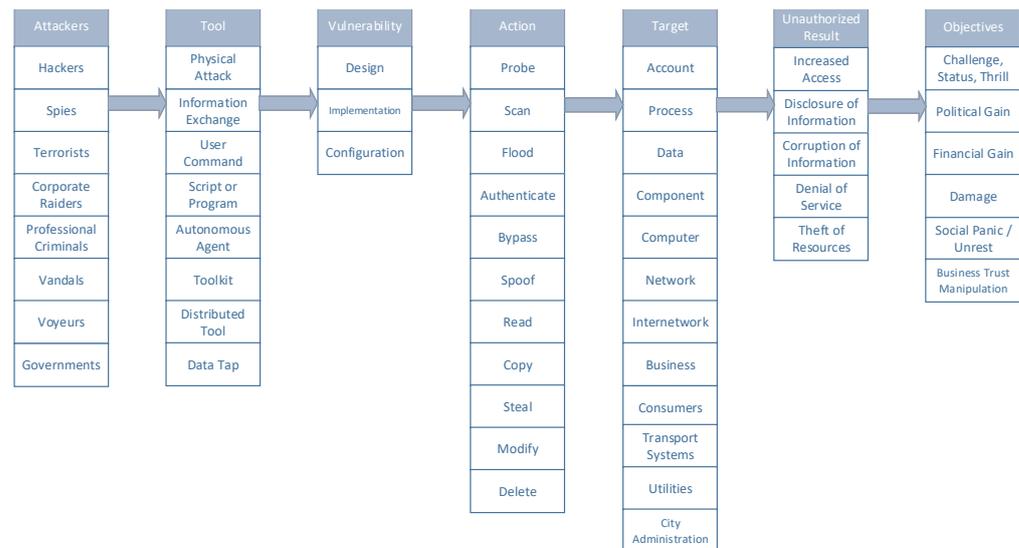


Figure 8. Modified CERT Attack Taxonomy for Smart Cities.

There are different types of security and privacy issues in IoT in Smart Cities, they exist on each of the three levels of the IoT architecture, application software layers, network layer and the perception layer along with some system wide issues, a discussion is provided for each of them. Furthermore, Table 14 provides a summary of the security and privacy issues in IoT for Smart Cities and the counter measures that one can take to mitigate them.

3.6.1. Application Software Layers (Middleware, Application and Business Layer)

Security and privacy in the application software layers tend to issues relating to storage of data and its usage. These are data visibility, access and injection.

Data Visibility/Identification

Once data is gathered, it is sent to the cloud where it is stored and mined to make inferences. Since the cloud would be used by multiple entities with different standards of security protocols and practices, it is extremely important that data stored in the cloud is encrypted so as not to allow its exposure to unwanted entities. Any data stored in plain form would be a risk to not only user privacy but also company rapport.

Data Access/Secondary Use

Access control is also a major issue in smart city data. Most Smart City applications rely on the usage of data from different applications to provide smart services, thus resulting in the gathered data to be used by many different enterprises. To allow this to take place smoothly while preserving privacy, suitable access control schemes will need to be devised to allow for responsible access to users of this data. A well-defined hierarchy of data users will need to be developed and implemented to limit access only to intended authorized personnel. Information flow control should also be employed that can track data flow as access to it is made and to detect any violation of access or usage rules. Moreover, data mashups that will occur in the cloud where multiple entities merge their data to work on some common goal, should be carried out with proper oversight. Data anonymization may also be required in such a scenario where specific values may be converted in to a range perhaps (e.g., using k-anonymity [224]) and unwanted data be deleted as necessary. Blockchain has been suggested to be used for access control as well as access tracking of users in IoT applications where each user access to a service or an application ends up as a transaction to form the applications IoT trail [232].

Data Injection/Data Integrity

Data injection refers to the injection of false information or modification information about a user in the system after gaining access. Since data is typically stored in databases, SQL injection involves an attacker inserting queries to modify data or make false data insertions into the database. This can have far reaching consequences for smart city applications such as patient record manipulation as well as manipulation or deletion of government records. SQL injection prevention schemes involve the validation of data before using it [233] such as positive pattern matching. It also involves limiting database access based on the user requirements and performing penetration testing.

3.6.2. Network Layer

Like other networks, the IoT in Smart Cities are also susceptible to network attacks such as Denial of service, Eavesdropping, Man in the middle attack, Side Channel and spoofing attacks [234]. We discuss these attacks and discuss remedial actions that should be taken to prevent them.

Man in the Middle Attack

Man in the middle (MITM) attack refers to the interception of data on the network by faking the identity of a network node or device. This is carried out by appearing as the intended recipient to the sender and the original sender to the recipient by unauthorized actors. To prevent this, the exchange of data between two entities should employ cryptographic protocols which can ensure secure communication. Many public networks do not make use of encryption when exchanging data, this endangers user data and can give access to unwanted persons to user information [224]. Policies need to be devised to allow for suitable data communication standards for such networks while keeping the user as well as commercial interests in mind.

Eavesdropping/Sniffing Attack

Eavesdropping refers to the listening of data on the network. In eavesdropping an unauthorized entity joins the network and can listen to the data that is being exchanged between the devices on the network. To avoid this, strategies include the use of authenticate always protocols which initiate authentication steps whenever devices need to communicate with each other. This will ensure that no unwanted users are allowed access to network traffic to prevent such attacks. Moreover, industry standard security protocols such as the TLS, WPA2 should be used for authenticating remote access. Furthermore, remote sessions should have time-outs implemented to ensure that mistakes are not made by forgetful employees.

Side Channel Attack

Side Channel Attacks refer to the extraction of information by observing operation characteristics of the implemented computer algorithms or systems such as power consumed, time taken, traffic analysis, fault analysis, acoustic analysis [235]. Side Channel attacks don't give nonpermitted parties access to the data within the network but may allow them to determine important information about the system, such as the protocol used, or allow them to drop packets so as to degrade performance of the network. One solution to counter network traffic side channels attacks is to saturate network bandwidth to prevent patterns from being observed. Another popular method of preventing side channel attacks is to make use of masking [236].

Denial of Service Attack

Denial of Service (DOS) or Distributed DOS attacks involve an entity getting access to the network and using legitimate nodes within it to flood the target with unnecessary requests to consume network bandwidth and degrade quality of service. With a smart city depending on sensors to provide it with a 'view' of the city, DOS attacks can make

the smart city system blind which can lead to loss of property and life. Countermeasures for DOS attacks involve anomaly detection by monitoring of network data to check for any irregular behavior. Artificial Intelligence has found applications in this area as noted by [237], for, e.g., it has been used to identify abnormal data in smart grids [238] as well as detecting attacks [239,240].

Spoofing Attack

In a spoofing attack, an attacker adds itself to the network by appearing to be a legitimate device on the network, thereby allowing them to send irregular or abnormal data to upset normal operation of a smart city system. Due to the varying nature and types of IoT devices having different levels of built-in security, spoofing is a particularly dangerous attack for IoT systems. Methods to prevent spoofing are the use of cryptography, hybrid encryption [241] as well as the use of blockchain [242] to validate data exchange and as well as authenticate devices.

3.6.3. Perception Layer

Perception layers attacks refer to physical attacks on an IoT based smart city system. This requires the physical presence of an attacker near the sensing elements in an IoT system. We cover these attacks to provide a holistic assessment of the security and privacy issues in IoT Smart Cities. Tempering and Radio Interference (jamming) are attacks which can affect the performance of smart city systems. Tempering may occur during the development or the manufacturing process while jamming can take place due to a generation of radio frequencies which interfere with the frequencies used by devices on the network to exchange data. To circumvent this, policies may be incorporated into software which alert businesses and other Smart City partners to missing or abnormal data from sensing devices.

3.6.4. System Wide Issues

Data Leakage

Data leakage refers to the unintentional conveyance of information about subjects in smart cities. The many data sources in smart cities may contain information related to a user's identity, health, quality of life etc. Smart City application managers use this data to improve their services and provide a better user experience, however, it is possible that this data might be shared with third party entities. It is therefore necessary to anonymize data before such assignments are taken. Data leakage can also take place when devices within a network perform discovery tasks and may provide personal information to rogue nodes in the network. In Smart Grids, power consumption data should be anonymized by considering the data on a neighborhood level rather than on the individual level, moreover, systems could be installed in homes using batteries to modify the demand response signal. Data aggregation is an important tool in preserving individual privacy and preventing data leakage. Moreover, data should be encrypted when sending it over the network so that any unauthorized access is avoided. Another strategy would be to use data minimization. Typically, sensors used in smart cities will gather data of less 'interest' in addition to data of interest. For, e.g., navigation systems many times record location information even when not in use or video applications such as facial recognition systems typically record other activities apart from being activated whenever a face is observed in the video. This extra information increases the risk of data leakage. Data minimization can be employed in such cases to limit the data that is being gathered on the user.

Trustworthiness

Apart from the technical steps that need to be taken to provide a secure usage experience of smart city applications and to encourage its use, it is important that smart city users be provided clear policy guidelines to how companies providing them these services will manage their data. Transparency in this regard will help increase user trust and the

feedback will enable companies to develop better data privacy mechanisms. Another way trust could be developed would be for the companies to provide customers who are vary of data collection, certain options in policies where they could choose which parts of the data collection are acceptable to them and which aren't.

Table 14. Security and Privacy issue for IoT Smart Cities.

Layer	Issue	Countermeasure
Application Software Layers (Middleware, Application and Business)	Data visibility/Identification Data access/Secondary use	- Use of encryption to store data - Access control schemes based on user hierarchy
	Data injection/Data integrity	- Data anonymization be employed - Use of blockchain for tracking user access - Use of data validation before usage - Limiting data access - Query parameterization - Penetration testing
Network Layer	Man in the middle attack	- Use of cryptographic protocols for data exchanges - Encrypting data on public networks
	Eavesdropping/Sniffing attack	- Use always authenticate protocols - Remote access should use industry accepted protocols such as TLS, WPA2
	Side channel attacks	- Timeouts for remote sessions - Bandwidth saturation
	Denial of Service	- Masking to prevent similar operational patterns - Check irregular data requests (AI has been shown to be of use here)
	Spoofing attacks	- Use of cryptography - Use of hybrid encryption - Use blockchain to validate data exchange as well as authenticate devices
Perception Layer System Wide	Tempering and Jamming Data leakage	- Software policies for missing data - Data anonymization - Data minimization - Data aggregation
	Trustworthiness	- Provide clear policy guidelines to users - Flexible policy development in consultation with users

4. SWOT Analysis

To complete this discussion, we perform a Strength Weaknesses Opportunities Threat (SWOT) analysis on the use of IoT for Smart Cities that discusses the strengths that IoT offers for Smart cities, the weaknesses in the current implementation scenario, the opportunities which exist for future work in this area as well as the threats that IoT application to smart cities faces, a summary of our discussion has been given in Table 15.

Table 15. SWOT Analysis for IoT in Smart Cities.

	Positive	Negative
Internal	Strengths - Sustainable living - Improved quality of life - Efficient city operations - Well suited for big data algorithms - Scalability of applications - Real-time/fast response due to distributed IoT structure - Reduced costs - Robustness - Enable heterogenous system connectivity	Weaknesses - Lack of data control policies - Laws need to be developed - Interoperability of networks - Incompatible sensor standards - Myriad of different application frameworks
	Opportunities - Development of new sensor technologies. - Development of low power and higher speed communication schemes - Development of Encryption techniques for storage and data exchange - Development of Data processing for privacy preservation techniques - Development of new city services - Development of scalable, explainable AI	Threats Trustworthiness issues among users - Network attacks - Data theft - Data leakage

4.1. Strengths

IoT smart city strengths are the fact that they provide an improved quality of life for a city's population along with reduction of costs in terms of operation and also enable cities

to be sustainable. IoT enables sensors and devices to be deployed throughout a city to give an overview of the state of the city's main functions such as transportation systems, electric, water and gas distribution as well as crime monitoring to name a few. This real time information helps city administration, businesses and other stakeholders to provide better services to people, increase the effectiveness of those services and reduce the cost through efficient operation.

On the technical side, IoT data has made possible to use data analytics to gauge various aspects of the multitude of services which are being provided in the city as well as to determine interactions between them and utilize that information for better decision making to make life easier for citizens. Furthermore, the distributed nature of IoT systems and the flexible architectures which enable fluidity through movement of sensing units is easily scalable thereby requiring little additional cost to upgrade and expand currently deployed systems. Moreover, this distributed architecture also makes such systems very robust to faults thereby increasing reliability of deployments and offering self-healing in applications such as electricity systems.

4.2. Weaknesses

IoT in Smart cities do suffer from some weaknesses in terms of technology, for, e.g., the current deployment scenario has a myriad of different technologies relating to networks, hardware platforms and software frameworks which do not often work together very well as discussed in the paper. Different standards' bodies such as the Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), the Institute of Electrical and Electronic Engineers (IEEE) and other organizations have been contributing with standards for communication, network discovery, identification, management of devices etc. However, the sheer number of 'standards' with many of them not being compatible with each other has not fully solved the interoperability problem and this can cause hurdles for expansion of IoT systems without a significant overhaul of system components. Another problem currently facing IoT systems is the lack of data policies and legislation. The concern here is that data policies are not mature enough to regulate how data is handled in IoT systems, as has been discussed previously. This is a major problem given the growing issue with user data privacy in a connected world.

4.3. Opportunities

IoT in Smart cities presents many opportunities to researchers and businesses alike in lieu of mitigating the weaknesses and also in the provision of new city services. The data gathered by the sensors in IoT systems has the potential to provide a holistic overview of the city's state allowing for the use of big data algorithms to develop new applications and services. For researchers in the data analytics domain, this heterogenous data provides a wonderful opportunity for the development of new data science algorithms for service delivery. There is a large monetary value towards the development and usage of computationally cheap encryption techniques, efficient data storage methods and networking technologies to make IoT deployment easier and cheaper. Development of new sensor technologies is another opportunity for researchers in IoT for smart cities. The development of newer, efficient, low-cost sensors would aid to the creation of IoT services and enable even wider usage.

4.4. Threats

With a connected system, there are several threats that come with IoTs for Smart Cities involving trust issues among users, privacy concerns due to network attacks, potential data theft etc. Privacy and security are the most important concerns of IoT applications, with such a personalized interaction mechanism between people and devices as is the case of smart cities, the risks for privacy breaches, data theft and leakages are high and this is a constant concern for service users as well as providers. Numerous attacks on Smart City systems have exposed the vulnerability of this technology to cyber attacks and

also demonstrated the consequences that it has on the population. Traditional security procedures and methods such as access authentication, routing and networking might not be enough or possible in many IoT deployments due to IoT devices typically not having sufficient computing capabilities, this has exacerbated the privacy and security concerns for IoT stakeholders. This can also feed to a lack of trust by customers to participate in smart city applications.

5. Conclusions

This paper presents a broad coverage of the Internet of Things in Smart Cities. Providing a detailed discussion of Smart Cities and its different domains, we present IoT as a vital enabler of smart city services and discuss the various smart city architectures and the challenges that are faced in the deployment of smart city applications. We follow this up with a review of the sensing and networking technologies used for such applications and discuss the usage of AI in smart cities. For each of the applications discussed for the various components, we have deliberated upon the type of deployment based on the technologies and architectures discussed to present an overview of the current research scenario in IoT based Smart Cities. Finally, the security and privacy issues faced by IoT based Smart Cities are discussed and a SWOT analysis is provided. It is envisaged that this survey will assist researchers by providing a comprehensive starting point to the use of IoT in Smart Cities. Table 16 provides a mapping of the papers cited in this survey to the survey outline provided in Figure 1.

Table 16. Mapping of Survey Sections to References.

Section	References
Smart Cities	[1–14]
Smart City Components [15]	[16,17,85–105]
Smart Agriculture	[18–21,106,107,107–120]
Smart City Services	[22,121–132]
Smart Energy	[23–25,133–154]
Smart Health	[155–169]
Smart Homes	[26–29,143,170–194]
Smart Industry	[30,31,195–204]
Smart Infrastructure	[32,32,205–221]
Smart Transport	[34]
IoT Architectures for Smart Cities [33]	[35,36]
Cloud Computing Model	[37,38]
Fog Computing Model	[9–11,22,39,47–51]
Edge Computing Model	[40,47]
Challenges	[10,33,41–44,47,52]
Smart Sensors	[8–11,45,46,46–50,222–242]
Networking	[53–55,55–58,58–66]
Big Data Analytics	[70–73]
Security and Privacy	[67,74–76]
Sensing Technologies	[11,77–82]
Networking Technologies [33,67,68]	[32,85,87–93,100–102,106,107,109,110,117–119,121–123,130,133,135,136,138–142,144,146–149,151,152,155,162,163,166,170–173,180,183,186,188,190,192,193,195,197,199,200,205,206,209,210,213,214,217,218,220]
Artificial Intelligence	[86,90,94–99,104,107,108,111–116,120,124–129,131,134,137,143,145,150,153,154,156–161,165,167,168,174–179,181,182,184,185,187,189,194,196,198,201–203,207,208,211,212,215,216,221]
Machine Learning	
Deep Learning	

6. Future Recommendations

From the discussion in this paper, there are several suggestions that can be made when using IoT for smart city projects. A major research area is in the security and privacy of IoT in smart cities in terms of encryption techniques, authentication protocols, data anonymization techniques and other methods to prevent unvalidated access to the IoT network. As mentioned before technologies such as blockchain could help introduce access tracking and control, secure device discovery, prevention of spoofing, data loss while ensuring that end to end encryption is also used.

Of the data transfer standards developed till now for IoT, most are not compatible with each other. Work needs to be carried out in this regard to enable intercommunication of sensor nodes using different protocols while utilizing low power, which is imperative for sensor nodes in the network.

Another area to work on, is the development of efficient storage techniques and low power hardware which can reduce operational costs. From a deployment perspective, decentralized systems have been proposed as the best solutions to increase reliability of the application. Techniques such as federated learning allow for decentralized DL system deployments.

The area of AI has a large scope for potential work too. This includes the development of data fusion techniques that can make the use of heterogeneous data sources easier, intelligent data reduction/feature selection methods to ensure that redundant or ‘uninteresting’ data is not part of the AI development pipeline. This will help in a quicker turnaround time as well as improved performance of deployments. Current methods need to be used as well as new ones be researched for making ML and DL algorithms more explainable to suit the various applications in a smart city.

Author Contributions: The review was conducted by A.S.S. under the guidance of D.S.-S., A.K. and A.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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.

References

1. Worldometers. World Population Forecast—Worldometers. 2019. Available online: <https://www.worldometers.info/world-population/world-population-projections/> (accessed on 9 March 2021)
2. Ahvenniemi, H.; Huovila, A.; Pinto-Seppä, I.; Airaksinen, M. What are the differences between sustainable and smart cities? *Cities* **2017**, *60*, 234–245. [CrossRef]
3. United Nations. About the Sustainable Development Goals—United Nations Sustainable Development. Available online: <https://sdgs.un.org/goals> (accessed on 9 March 2021)
4. Cardullo, P.; Kitchin, R. Being a ‘citizen’ in the smart city: Up and down the scaffold of smart citizen participation in Dublin, Ireland. *GeoJournal* **2019**, *84*, 1–13. [CrossRef]
5. Desdemoustier, J.; Crutzen, N.; Giffinger, R. Municipalities’ understanding of the Smart City concept: An exploratory analysis in Belgium. *Technol. Forecast. Soc. Chang.* **2019**, *142*, 129–141. [CrossRef]
6. Khan, M.S.; Woo, M.; Nam, K.; Chathoth, P.K. Smart city and smart tourism: A case of Dubai. *Sustainability* **2017**, *9*, 2279. [CrossRef]
7. Wu, S.M.; Chen, T.C.; Wu, Y.J.; Lytras, M. Smart cities in Taiwan: A perspective on big data applications. *Sustainability* **2018**, *10*, 106. [CrossRef]
8. Ejaz, W.; Anpalagan, A. Internet of things for smart cities: Overview and key challenges. *Internet Things Smart Cities* **2019**, 1–15. [CrossRef]
9. Janssen, M.; Luthra, S.; Mangla, S.; Rana, N.P.; Dwivedi, Y.K. Challenges for adopting and implementing IoT in smart cities: An integrated MICMAC-ISM approach. *Internet Res.* **2019**, *29*, 1589–1616. [CrossRef]
10. Sánchez-Corcuera, R.; Nuñez-Marcos, A.; Sesma-Solance, J.; Bilbao-Jayo, A.; Mulero, R.; Zulaika, U.; Azkune, G.; Almeida, A. Smart cities survey: Technologies, application domains and challenges for the cities of the future. *Int. J. Distrib. Sens. Netw.* **2019**, *15*. [CrossRef]
11. Silva, B.N.; Khan, M.; Han, K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustain. Cities Soc.* **2018**, *38*, 697–713. [CrossRef]
12. Atat, R.; Liu, L.; Wu, J.; Li, G.; Ye, C.; Yang, Y. Big data meet cyber-physical systems: A panoramic survey. *IEEE Access* **2018**, *6*, 73603–73636. [CrossRef]
13. Hollands, R.G. Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City* **2008**, *12*, 303–320. [CrossRef]
14. Anthopoulos, L.G.; Reddick, C.G. Understanding electronic government research and smart city: A framework and empirical evidence. *Inf. Polity* **2016**, *21*, 99–117. [CrossRef]

15. Khan, Z.; Anjum, A.; Soomro, K.; Tahir, M.A. Towards cloud based big data analytics for smart future cities. *J. Cloud Comput.* **2015**, *4*. [[CrossRef](#)]
16. Koubaa, A.; Aldawood, A.; Saeed, B.; Hadid, A.; Ahmed, M.; Saad, A.; Alkhouja, H.; Ammar, A.; Alkanhal, M. Smart palm: An IoT framework for red palm weevil early detection. *Agronomy* **2020**, *10*, 987. [[CrossRef](#)]
17. O'Grady, M.; Langton, D.; O'Hare, G. Edge computing: A tractable model for smart agriculture? *Artif. Intell. Agric.* **2019**, *3*, 42–51. [[CrossRef](#)]
18. Rojek, I.; Studzinski, J. Detection and localization of water leaks in water nets supported by an ICT system with artificial intelligence methods as away forward for smart cities. *Sustainability* **2019**, *11*, 518. [[CrossRef](#)]
19. Pardini, K.; Rodrigues, J.J.; Kozlov, S.A.; Kumar, N.; Furtado, V. IoT-based solid waste management solutions: A survey. *J. Sens. Actuator Netw.* **2019**, *8*, 5. [[CrossRef](#)]
20. Dutta, J.; Chowdhury, C.; Roy, S.; Middy, A.I.; Gazi, F. Towards smart city: Sensing air quality in city based on opportunistic crowd-sensing. *ACM Int. Conf. Proc. Ser.* **2017**. [[CrossRef](#)]
21. Al-Turjman, F.; Malekloo, A. Smart parking in IoT-enabled cities: A survey. *Sustain. Cities Soc.* **2019**, *49*. [[CrossRef](#)]
22. Shirazi, E.; Jadid, S. Autonomous Self-healing in Smart Distribution Grids Using Multi Agent Systems. *IEEE Trans. Ind. Informatics* **2018**, *3203*, 1–11. [[CrossRef](#)]
23. Andreão, R.V.; Athayde, M.; Boudy, J.; Aguilar, P.; de Araujo, I.; Andrade, R. Raspcare: A Telemedicine Platform for the Treatment and Monitoring of Patients with Chronic Diseases. In *Assistive Technologies in Smart Cities*; IntechOpen: London, UK, 2018.
24. Keane, P.A.; Topol, E.J. With an eye to AI and autonomous diagnosis. *NPJ Digit. Med.* **2018**, *1*, 10–12. [[CrossRef](#)] [[PubMed](#)]
25. Trencher, G.; Karvonen, A. Stretching “smart”: Advancing health and well-being through the smart city agenda. *Local Environ.* **2019**, *24*, 610–627. [[CrossRef](#)]
26. Haverkort, B.R.; Zimmermann, A. Smart Industry: How ICT Will Change the Game! *IEEE Internet Comput.* **2017**, *21*, 8–10. [[CrossRef](#)]
27. Tao, F.; Cheng, J.; Qi, Q. IIHub: An industrial internet-of-things hub toward smart manufacturing based on cyber-physical system. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2271–2280. [[CrossRef](#)]
28. Trakadas, P.; Simoens, P.; Gkonis, P.; Sarakis, L.; Angelopoulos, A.; Ramallo-González, A.P.; Skarmeta, A.; Trochoutsos, C.; Calvo, D.; Pariente, T.; et al. An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. *Sensors* **2020**, *20*, 5480. [[CrossRef](#)]
29. Wan, J.; Yang, J.; Wang, Z.; Hua, Q. Artificial intelligence for cloud-assisted smart factory. *IEEE Access* **2018**, *6*, 55419–55430. [[CrossRef](#)]
30. Huang, Y.; Dang, Z.; Choi, Y.; Andrade, J.; Bar-ilan, A. High-precision smart system on accelerometers and inclinometers for Structural Health Monitoring: Development and applications. In *Proceedings of the 2018 12th France-Japan and 10th Europe-Asia Congress on Mechatronics*, Tsu, Japan, 10–12 September 2018; pp. 52–57.
31. Farag, S.G. Application of Smart Structural System for Smart Sustainable Cities. In *Proceedings of the 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, Muscat, Oman, 15–16 January 2019; pp. 1–5. [[CrossRef](#)]
32. Wang, Y.; Ram, S.; Currim, F.; Dantas, E.; Sabóia, L.A. A big data approach for smart transportation management on bus network. In *Proceedings of the IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life, ISC2 2016—Proceedings*, Trento, Italy, 12–15 September 2016; pp. 1–6. [[CrossRef](#)]
33. Lele, A. Internet of things (IoT). *Smart Innov. Syst. Technol.* **2019**, *132*, 187–195. [[CrossRef](#)]
34. Mell, P.; Grance, T. *The NIST-National Institute of Standards and Technology- Definition of Cloud Computing*; NIST Special Publication 800-145; NIST: Gaithersburg, MD, USA, 2011;
35. Bar-Magen Numhauser, J. *Fog Computing Introduction to a New Cloud Evolution*; University of Alcalá: Alcalá de Henares, Spain, 2012.
36. Aazam, M.; Zeadally, S.; Harras, K.A. Fog Computing Architecture, Evaluation, and Future Research Directions. *IEEE Commun. Mag.* **2018**, *56*, 46–52. [[CrossRef](#)]
37. El-Sayed, H.; Sankar, S.; Prasad, M.; Puthal, D.; Gupta, A.; Mohanty, M.; Lin, C.T. Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment. *IEEE Access* **2017**, *6*, 1706–1717. [[CrossRef](#)]
38. Yousefpour, A.; Fung, C.; Nguyen, T.; Kadiyala, K.; Jalali, F.; Niakanlahiji, A.; Kong, J.; Jue, J.P. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *J. Syst. Archit.* **2019**, *98*, 289–330. [[CrossRef](#)]
39. Risteska Stojkoska, B.L.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [[CrossRef](#)]
40. Saini, A.; Malik, A. Routing in internet of things: A survey. *Commun. Comput. Syst.* **2017**, *1*, 855–860. [[CrossRef](#)]
41. Casilari, E.; Lora-rivera, R.; García-lagos, F. A study on the application of convolutional neural networks to fall detection evaluated with multiple public datasets. *Sensors* **2020**, *20*, 1466. [[CrossRef](#)] [[PubMed](#)]
42. Rahneemofar, M.; Sheppard, C. Deep count: Fruit counting based on deep simulated learning. *Sensors* **2017**, *17*, 905. [[CrossRef](#)] [[PubMed](#)]
43. Thakker, D.; Mishra, B.K.; Abdullatif, A.; Mazumdar, S. Explainable Artificial Intelligence for Developing Smart Cities Solutions. *Smart Cities* **2020**, *3*, 1353–1382. [[CrossRef](#)]
44. Rahman, A.; Hossain, M.S.; Alrajeh, N.A.; Guizani, N. B5G and Explainable Deep Learning Assisted Healthcare Vertical at the Edge: COVID-19 Perspective. *IEEE Netw.* **2020**, *34*, 98–105. [[CrossRef](#)]

45. Marques, G.; Garcia, N.; Pombo, N. A survey on IoT: architectures, elements, applications, QoS, platforms and security concepts. In *Advances in Mobile Cloud Computing and Big Data in the 5G Era*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 115–130.
46. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [[CrossRef](#)]
47. Mehmood, Y.; Ahmad, F.; Yaqoob, I.; Adnane, A.; Imran, M.; Guizani, S. Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. *IEEE Commun. Mag.* **2017**, *55*, 16–24. [[CrossRef](#)]
48. Rong, W.; Xiong, Z.; Cooper, D.; Li, C.; Sheng, H. Smart city architecture: A technology guide for implementation and design challenges. *China Commun.* **2014**, *11*, 56–69. [[CrossRef](#)]
49. Ahmed, E.; Yaqoob, I.; Gani, A.; Imran, M.; Guizani, M. Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges. *IEEE Wirel. Commun.* **2016**, *23*, 10–16. [[CrossRef](#)]
50. Chen, S.; Xu, H.; Liu, D.; Hu, B.; Wang, H. A vision of IoT: Applications, challenges, and opportunities with China Perspective. *IEEE Internet Things J.* **2014**, *1*, 349–359. [[CrossRef](#)]
51. Ahlgren, B.; Hidell, M.; Ngai, E.C. Internet of Things for Smart Cities: Interoperability and Open Data. *IEEE Internet Comput.* **2016**, *20*, 52–56. [[CrossRef](#)]
52. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Bus. Horizons* **2015**, *58*, 431–440. [[CrossRef](#)]
53. Morais, C.M.; Sadok, D.; Kelner, J. An IoT sensor and scenario survey for data researchers. *J. Braz. Comput. Soc.* **2019**, *25*. [[CrossRef](#)]
54. Sharma, N.; Solanki, V.K.; Davim, J.P. Basics of the Internet of Things (IoT) and Its Future. In *Handbook of IoT and Big Data*; CRC Press: Boca Raton, FL, USA, **2019**; p. 165.
55. Hancke, G.P.; Hancke, G.P., Jr. The role of advanced sensing in smart cities. *Sensors* **2013**, *13*, 393–425. [[CrossRef](#)] [[PubMed](#)]
56. Penza, M.; Suriano, D.; Villani, M.G.; Spinelle, L.; Gerboles, M. Towards air quality indices in smart cities by calibrated low-cost sensors applied to networks. In Proceedings of the SENSORS, 2014 IEEE, Valencia, Spain, 2–5 November 2014; pp. 2012–2017.
57. Foliato, F.; Low, Y.S.; Yeow, W.L. Smartbin: Smart waste management system. In Proceedings of the 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, 7–9 April 2015; pp. 1–2.
58. Bedi, G.; Venayagamoorthy, G.K.; Singh, R.; Brooks, R.R.; Wang, K.C. Review of Internet of Things (IoT) in Electric Power and Energy Systems. *IEEE Internet Things J.* **2018**, *5*, 847–870. [[CrossRef](#)]
59. Song, E.Y.; Fitzpatrick, G.J.; Lee, K.B. Smart Sensors and Standard-Based Interoperability in Smart Grids. *IEEE Sens. J.* **2017**, *17*, 7723–7730. [[CrossRef](#)]
60. Abdellatif, A.A.; Mohamed, A.; Chiasserini, C.F.; Tlili, M.; Erbad, A. Edge computing for smart health: Context-aware approaches, opportunities, and challenges. *IEEE Netw.* **2019**, *33*, 196–203. [[CrossRef](#)]
61. Fan, K.; Zhu, S.; Zhang, K.; Li, H.; Yang, Y. A Lightweight Authentication Scheme for Cloud-Based RFID Healthcare Systems. *IEEE Netw.* **2019**, *33*, 44–49. [[CrossRef](#)]
62. Prati, A.; Shan, C.; Wang, K.I. Sensors, vision and networks: From video surveillance to activity recognition and health monitoring. *J. Ambient. Intell. Smart Environ.* **2019**, *11*, 5–22. [[CrossRef](#)]
63. Ding, D.; Cooper, R.A.; Pasquina, P.F.; Fici-Pasquina, L. Sensor technology for smart homes. *Maturitas* **2011**, *69*, 131–136. [[CrossRef](#)] [[PubMed](#)]
64. Jan, B.; Farman, H.; Khan, M.; Talha, M.; Din, I.U. Designing a Smart Transportation System: An Internet of Things and Big Data Approach. *IEEE Wirel. Commun.* **2019**, *26*, 73–79. [[CrossRef](#)]
65. Guerrero-Ibáñez, J.; Zeadally, S.; Contreras-Castillo, J. Sensor technologies for intelligent transportation systems. *Sensors* **2018**, *18*, 1212. [[CrossRef](#)]
66. Gharaibeh, A.; Salahuddin, M.A.; Hussini, S.J.; Khreishah, A.; Khalil, I.; Guizani, M.; Al-Fuqaha, A. Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2456–2501. [[CrossRef](#)]
67. Talari, S.; Shafie-Khah, M.; Siano, P.; Loia, V.; Tommasetti, A.; Catalão, J.P. A review of smart cities based on the internet of things concept. *Energies* **2017**, *10*, 421. [[CrossRef](#)]
68. Park, D.M.; Kim, S.K.; Seo, Y.S. S-mote: SMART home framework for common household appliances in IoT Network. *J. Inf. Process. Syst.* **2019**, *15*, 449–456. [[CrossRef](#)]
69. Yaqoob, I.; Ahmed, E.; Hashem, I.A.T.; Ahmed, A.I.A.; Gani, A.; Imran, M.; Guizani, M. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE Wirel. Commun.* **2017**, *24*, 10–16. [[CrossRef](#)]
70. Sakhardande, P.; Hanagal, S.; Kulkarni, S. Design of disaster management system using IoT based interconnected network with smart city monitoring. In Proceedings of the 2016 International Conference on Internet of Things and Applications, IOTA 2016, Pune, India, 22–24 January 2016; pp. 185–190. [[CrossRef](#)]
71. Kang, L.; Poslad, S.; Wang, W.; Li, X.; Zhang, Y.; Wang, C. A public transport bus as a flexible mobile smart environment sensing platform for IoT. In Proceedings of the 12th International Conference on Intelligent Environments, IE 2016, London, UK, 14–16 September 2016; pp. 1–8. [[CrossRef](#)]
72. Adiono, T.; Fathany, M.Y.; Putra, R.V.W.; Afifah, K.; Santrijaji, M.H.; Lawu, B.L.; Fuada, S. Live demonstration: MINDS - Meshed and internet networked devices system for smart home: Track selection: Embedded systems. In Proceedings of the 2016 IEEE Asia Pacific Conference on Circuits and Systems, APCCAS 2016, Jeju, Korea, 25–28 October 2016; pp. 736–737. [[CrossRef](#)]

73. Ghosh, A.; Chakraborty, N. Design of smart grid in an University Campus using ZigBee mesh networks. In Proceedings of the 1st IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems, ICPEICES 2016, Delhi, India, 4–6 July 2016; pp. 1–6. [CrossRef]
74. Yan, Y.; Qian, Y.; Sharif, H. A secure data aggregation and dispatch scheme for home area networks in smart grid. In Proceedings of the GLOBECOM—IEEE Global Telecommunications Conference, Houston, TX, USA, 5–9 December 2011; pp. 1–6. [CrossRef]
75. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low Power Wide Area Networks: An Overview. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 855–873. [CrossRef]
76. Kuzlu, M.; Pipattanasomporn, M. Assessment of communication technologies and network requirements for different smart grid applications. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference, ISGT 2013, Washington, DC, USA, 24–27 February 2013; pp. 1–6. [CrossRef]
77. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols: Review. In Proceedings of the ICIT 2017—8th International Conference on Information Technology, Amman, Jordan, 17–18 May 2017; pp. 685–690. [CrossRef]
78. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **2019**, *5*, 1–7. [CrossRef]
79. Samuel, S.S.I. A review of connectivity challenges in IoT-smart home. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City, ICBDS 2016, Muscat, Oman, 15–16 March 2016, pp. 364–367. [CrossRef]
80. Kuppusamy, P.; Muthuraj, S.; Gopinath, S. Survey and challenges of Li-Fi with comparison of Wi-Fi. In Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 23–25 March 2016; pp. 896–899.
81. Heile, B.S.A.; Liu, B.; Zhang, M.; Perkins, C.F. Wi-SUN FAN Overview. 2017. Available online: <https://tools.ietf.org/id/draft-heile-lpwan-wisun-overview-00.html> (accessed on 9 March 2021)
82. Hammi, B.; Khatoun, R.; Zeadally, S.; Fayad, A.; Khoukhi, L. IoT technologies for smart cities. *IET Netw.* **2018**, *7*, 1–13. [CrossRef]
83. de Souza, J.T.; de Francisco, A.C.; Piekarski, C.M.; do Prado, G.F. Data mining and machine learning to promote smart cities: A systematic review from 2000 to 2018. *Sustainability* **2019**, *11*, 1077. [CrossRef]
84. Rayan, Z.; Alfonse, M.; Salem, A.B.M. Machine Learning Approaches in Smart Health. *Procedia Comput. Sci.* **2018**, *154*, 361–368. [CrossRef]
85. Varghese, R.; Sharma, S. Affordable smart farming using IoT and machine learning. In Proceedings of the 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 14–15 June 2018; pp. 645–650.
86. AlZu'bi, S.; Hawashin, B.; Mujahed, M.; Jararweh, Y.; Gupta, B.B. An efficient employment of internet of multimedia things in smart and future agriculture. *Multimed. Tools Appl.* **2019**, *78*, 29581–29605. [CrossRef]
87. Pratyush Reddy, K.S.; Roopa, Y.M.; Kovvada Rajeev, L.N.; Nandan, N.S. IoT based Smart Agriculture using Machine Learning. In Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020, Coimbatore, India, 15–17 July 2020; pp. 130–134. [CrossRef]
88. Goap, A.; Sharma, D.; Shukla, A.K.; Rama Krishna, C. An IoT based smart irrigation management system using Machine learning and open source technologies. *Comput. Electron. Agric.* **2018**, *155*, 41–49. [CrossRef]
89. Rodríguez, S.; Gualotuña, T.; Grilo, C. A System for the Monitoring and Predicting of Data in Precision A Agriculture System for the and Predicting of Wireless Data in Precision in a Monitoring Rose Greenhouse Based on Sensor Agriculture in a Rose Greenhouse Based on Wireless Sensor Networks Ne. *Procedia Comput. Sci.* **2017**, *121*, 306–313. [CrossRef]
90. Kitpo, N.; Kugai, Y.; Inoue, M.; Yokemura, T.; Satomura, S. Internet of Things for Greenhouse Monitoring System Using Deep Learning and Bot Notification Services. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics, ICCE 2019, Las Vegas, NV, USA, 11–13 January 2019. [CrossRef]
91. Saha, A.K.; Saha, J.; Ray, R.; Sircar, S.; Dutta, S.; Chattopadhyay, S.P.; Saha, H.N. IOT-based drone for improvement of crop quality in agricultural field. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 612–615.
92. Araby, A.A.; Abd Elhameed, M.M.; Magdy, N.M.; Abdelaal, N.; Abd Allah, Y.T.; Darweesh, M.S.; Fahim, M.A.; Mostafa, H. Smart iot monitoring system for agriculture with predictive analysis. In Proceedings of the 2019 8th International Conference on Modern Circuits and Systems Technologies (MOCAS), Thessaloniki, Greece, 13–15 May 2019; pp. 1–4.
93. Nandhini, S.A.; Radha, R.H.S. Web Enabled Plant Disease Detection System for Agricultural Applications Using WMSN. *Wirel. Pers. Commun.* **2018**, *102*, 725–740. [CrossRef]
94. Ale, L.; Sheta, A.; Li, L.; Wang, Y.; Zhang, N. Deep learning based plant disease detection for smart agriculture. In Proceedings of the 2019 IEEE Globecom Workshops, GC Wkshps 2019—Proceedings, Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [CrossRef]
95. Balducci, F.; Impedovo, D.; Pirlo, G. Machine learning applications on agricultural datasets for smart farm enhancement. *Machines* **2018**, *6*, 38. [CrossRef]
96. Jin, X.B.; Yang, N.X.; Wang, X.Y.; Bai, Y.T.; Su, T.L.; Kong, J.L. Hybrid deep learning predictor for smart agriculture sensing based on empirical mode decomposition and gated recurrent unit group model. *Sensors* **2020**, *20*, 1334. [CrossRef]

97. Aruul Mozhi Varman, S.; Baskaran, A.R.; Aravindh, S.; Prabhu, E. Deep Learning and IoT for Smart Agriculture Using WSN. In Proceedings of the 2017 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2017, Tamil Nadu, India, 14–16 December 2017, pp. 1–6. [\[CrossRef\]](#)
98. Jin, X.B.; Yu, X.H.; Wang, X.Y.; Bai, Y.T.; Su, T.L.; Kong, J.L. Deep learning predictor for sustainable precision agriculture based on internet of things system. *Sustainability* **2020**, *12*, 1433. [\[CrossRef\]](#)
99. Aliev, K.; Jawaid, M.M.; Narejo, S.; Pasero, E.; Pulatov, A. Internet of plants application for smart agriculture. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 421–429. [\[CrossRef\]](#)
100. Diedrichs, A.L.; Bromberg, F.; Dujovne, D.; Brun-Laguna, K.; Watteyne, T. Prediction of frost events using machine learning and IoT sensing devices. *IEEE Internet Things J.* **2018**, *5*, 4589–4597. [\[CrossRef\]](#)
101. Reshma, R.; Sathiyavathi, V.; Sindhu, T.; Selvakumar, K.; SaiRamesh, L. IoT based Classification Techniques for Soil Content Analysis and Crop Yield Prediction. In Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 7–9 October 2020; pp. 156–160.
102. Pawar, M.; Chillarge, G. Soil toxicity prediction and recommendation system using data mining in precision agriculture. In Proceedings of the 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 6–8 April 2018; pp. 1–5.
103. Lee, K.; Silva, B.N.; Han, K. Deep learning entrusted to fog nodes (DLEFN) based smart agriculture. *Appl. Sci.* **2020**, *10*, 1544. [\[CrossRef\]](#)
104. Guillén, M.A.; Llanes, A.; Imberón, B.; Martínez, R.; Andrés, E.; Crespo, B.; Carlos, J. Performance evaluation of edge computing platforms for the prediction of low temperatures in agriculture using deep learning. *J. Supercomput.* **2021**, *77*, 818–840. [\[CrossRef\]](#)
105. Guillén-Navarro, M.A.; Martínez-España, R.; López, B.; Cecilia, J.M. A high-performance IoT solution to reduce frost damages in stone fruits. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e5299. [\[CrossRef\]](#)
106. Rutqvist, D.; Kleyko, D.; Blomstedt, F. An Automated Machine Learning Approach for Smart Waste Management Systems. *IEEE Trans. Ind. Informatics* **2019**. [\[CrossRef\]](#)
107. Hussain, A.; Draz, U.; Ali, T.; Tariq, S.; Irfan, M.; Glowacz, A.; Antonino Daviu, J.A.; Yasin, S.; Rahman, S. Waste Management and Prediction of Air Pollutants Using IoT and Machine Learning Approach. *Energies* **2020**, *13*, 3930. [\[CrossRef\]](#)
108. Zhang, D.; Lindholm, G.; Ratnaweera, H. Use long short-term memory to enhance Internet of Things for combined sewer overflow monitoring. *J. Hydrol.* **2018**, *556*, 409–418. [\[CrossRef\]](#)
109. Varalakshmi, P.; Vandhana, S.; Vishali, S. Prediction of water quality using Naive Bayesian algorithm. In Proceedings of the 2016 8th International Conference on Advanced Computing, ICoAC 2016, Tamil Nadu, India, 19–21 January 2016; pp. 224–229. [\[CrossRef\]](#)
110. Jalal, D. Toward a Smart Real Time Monitoring System for Drinking Water Based on Machine Learning. In Proceedings of the 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 19–21 September 2019; pp. 1–5.
111. Bin, T.; Alam, M.M.; Absar, N.; Andersson, K.; Shahadat, M. IoT Based Real-time River Water Quality Monitoring System. *Procedia Comput. Sci.* **2019**, *155*, 161–168. [\[CrossRef\]](#)
112. Liu, P.; Wang, J.; Sangaiah, A.K.; Xie, Y.; Yin, X. Analysis and prediction of water quality using LSTM deep neural networks in IoT environment. *Sustainability* **2019**, *11*, 2058. [\[CrossRef\]](#)
113. Tariq, Z.; Shah, S.K.; Lee, Y. Smart 311 Request System with Automatic Noise Detection for Safe Neighborhood. In Proceedings of the 2018 IEEE International Smart Cities Conference, ISC2 2018, Kansas City, MO, USA, 16–19 September 2018; pp. 1–8. [\[CrossRef\]](#)
114. Zhang, X.; Zhao, M.; Dong, R. Time-series prediction of environmental noise for urban iot based on long short-term memory recurrent neural network. *Appl. Sci.* **2020**, *10*, 1144. [\[CrossRef\]](#)
115. Santur, Y.; Karaköse, E.; Karaköse, M.; Akin, E. Deep Learning Based Artificial Manager for Smart City. In Proceedings of the 5th International Conference on Advanced Technology & Sciences, Istanbul, Turkey, 9–12 May 2017; pp. 197–201.
116. Sanaei, S.; Majidi, B.; Akhtarkavan, E. Deep Multisensor Dashboard for Composition Layer of Web of Things in the Smart City. In Proceedings of the 9th International Symposium on Telecommunication: With Emphasis on Information and Communication Technology, IST 2018, Tehran, Iran, 17–19 December 2018; pp. 211–215. [\[CrossRef\]](#)
117. Rosero-Montalvo, P.D.; Caraguay-Procel, J.A.; Jaramillo, E.D.; Michilena-Calderon, J.M.; Umaquina-Criollo, A.C.; Mediavilla-Valverde, M.; Ruiz, M.A.; Beltran, L.A.; Peluffo-Ordóñez, D.H. Air quality monitoring intelligent system using machine learning techniques. In Proceedings of the 3rd International Conference on Information Systems and Computer Science, INCISCOS 2018, Quito, Ecuador, 14–16 November 2018; pp. 75–80. [\[CrossRef\]](#)
118. Feng, C.; Wang, W.; Tian, Y.; Que, X.; Gong, X. Estimate Air Quality Based on Mobile Crowd Sensing and Big Data. In Proceedings of the 18th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2017—Conference, Macau, China, 12–15 June 2017. [\[CrossRef\]](#)
119. Yu, R.; Yang, Y.; Yang, L.; Han, G.; Move, O.A. RAQ—A random forest approach for predicting air quality in urban sensing systems. *Sensors* **2016**, *16*, 86. [\[CrossRef\]](#)
120. Kök, I.; Şimşek, M.U.; Özdemir, S. A deep learning model for air quality prediction in smart cities. In Proceedings of the Proceedings—2017 IEEE International Conference on Big Data, Big Data 2017, Boston, MA, USA, 11–14 December 2017; pp. 1983–1990. [\[CrossRef\]](#)

121. Al-Wakeel, A.; Wu, J.; Jenkins, N. K-Means Based Load Estimation of Domestic Smart Meter Measurements. *Appl. Energy* **2017**, *194*, 333–342. [[CrossRef](#)]
122. Valgaev, O.; Kupzog, F.; Schmeck, H. Building power demand forecasting using K-nearest neighbours model—Practical application in Smart City Demo Aspern project. *CIREN—Open Access Proc. J.* **2017**, *2017*, 1601–1604. [[CrossRef](#)]
123. Vrablcová, P.; Bou Ezzeddine, A.; Rozinajová, V.; Šárik, S.; Sangaiah, A.K. Smart grid load forecasting using online support vector regression. *Comput. Electr. Eng.* **2018**, *65*, 102–117. [[CrossRef](#)]
124. Kong, W.; Dong, Z.Y.; Jia, Y.; Hill, D.J.; Xu, Y.; Zhang, Y. Short-Term Residential Load Forecasting Based on LSTM Recurrent Neural Network. *IEEE Trans. Smart Grid* **2019**, *10*, 841–851. [[CrossRef](#)]
125. Hosein, S.; Hosein, P. Load forecasting using deep neural networks. In Proceedings of the 2017 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2017, Washington, DC, USA, 23–26 April 2017. [[CrossRef](#)]
126. Ke, K.; Hongbin, S.; Chengkang, Z.; Brown, C. Short-term electrical load forecasting method based on stacked auto-encoding and GRU neural network. *Evol. Intell.* **2019**, *12*, 385–394. [[CrossRef](#)]
127. Han, T.; Muhammad, K.; Hussain, T.; Lloret, J.; Baik, S.W. An Efficient Deep Learning Framework for Intelligent Energy Management in IoT Networks. *IEEE Internet Things J.* **2020**. [[CrossRef](#)]
128. Liu, X.; Xiao, Z.; Zhu, R.; Wang, J.; Liu, L.; Ma, M. Edge sensing data-imaging conversion scheme of load forecasting in smart grid. *Sustain. Cities Soc.* **2020**, *62*, 102363. [[CrossRef](#)]
129. Taïk, A.; Cherkaoui, S. Electrical load forecasting using edge computing and federated learning. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
130. Nguyen, D.; Barella, R.; Wallace, S.A.; Zhao, X.; Liang, X. Smart grid line event classification using supervised learning over PMU data streams. In Proceedings of the 2015 6th International Green and Sustainable Computing Conference, Las Vegas, NV, USA, 14–16 December 2015. [[CrossRef](#)]
131. Zheng, Z.; Yang, Y.; Niu, X.; Dai, H.N.; Zhou, Y. Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids. *IEEE Trans. Ind. Infor.* **2018**, *14*, 1606–1615. [[CrossRef](#)]
132. Huang, Y.; Lu, Y.; Wang, F.; Fan, X.; Liu, J.; Leung, V.C. An edge computing framework for real-time monitoring in smart grid. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA, 21–23 October 2018; pp. 99–108.
133. Batool, S.; Saqib, N.A.; Khan, M.A. Internet of Things data analytics for user authentication and activity recognition. In Proceedings of the 2017 2nd International Conference on Fog and Mobile Edge Computing, FMEC 2017, Valencia, Spain, 8–11 May 2017; pp. 183–187. [[CrossRef](#)]
134. Zhang, H.; Xiao, Z.; Wang, J.; Li, F.; Szczerbicki, E. A novel IoT-perceptive human activity recognition (HAR) approach using multihead convolutional attention. *IEEE Internet Things J.* **2019**, *7*, 1072–1080. [[CrossRef](#)]
135. Castro, D.; Coral, W.; Rodriguez, C.; Cabra, J.; Colorado, J. Wearable-based human activity recognition using an iot approach. *J. Sens. Actuator Netw.* **2017**, *6*, 28. [[CrossRef](#)]
136. Tran, D.N.; Phan, D.D. Human Activities Recognition in Android Smartphone Using Support Vector Machine. In Proceedings of the International Conference on Intelligent Systems, Modelling and Simulation, ISMS, Bangkok, Thailand, 25–27 January 2016; pp. 64–68. [[CrossRef](#)]
137. Santos, G.L.; Endo, P.T.; Monteiro, K.H.d.C.; Rocha, E.d.S.; Silva, I.; Lynn, T. Accelerometer-based human fall detection using convolutional neural networks. *Sensors* **2019**, *19*, 1644. [[CrossRef](#)]
138. Yacchirema, D.; de Puga, J.S.; Palau, C.; Esteve, M. Fall detection system for elderly people using IoT and ensemble machine learning algorithm. *Pers. Ubiquitous Comput.* **2019**, *23*, 801–817. [[CrossRef](#)]
139. Machorro-Cano, I.; Alor-Hernández, G.; Paredes-Valverde, M.A.; Ramos-Deonati, U.; Sánchez-Cervantes, J.L.; Rodríguez-Mazahua, L. PISIoT: A machine learning and IoT-based smart health platform for overweight and obesity control. *Appl. Sci.* **2019**, *9*, 3037. [[CrossRef](#)]
140. Ani, R.; Krishna, S.; Anju, N.; Sona, A.M.; Deepa, O.S. IoT based patient monitoring and diagnostic prediction tool using ensemble classifier. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017, Udipi (Near Mangalore), India, 13–16 September 2017; pp. 1588–1593. [[CrossRef](#)]
141. Ukil, A.; Roy, U.K. Smart cardiac health management in iot through heart sound signal analytics and robust noise filtering. In Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, Montreal, QC, Canada, 8–13 October 2017; pp. 1–5. [[CrossRef](#)]
142. Alamri, A. Monitoring System for Patients Using Multimedia for Smart Healthcare. *IEEE Access* **2018**, *6*, 23271–23276. [[CrossRef](#)]
143. Qu, Y.; Ming, X.; Qiu, S.; Zheng, M.; Hou, Z. An integrative framework for online prognostic and health management using internet of things and convolutional neural network. *Sensors* **2019**, *19*, 2338. [[CrossRef](#)] [[PubMed](#)]
144. Hossain, M.S.; Muhammad, G. Cloud-assisted Industrial Internet of Things (IIoT)—Enabled framework for health monitoring. *Comput. Netw.* **2016**, *101*, 192–202. [[CrossRef](#)]
145. Alhussein, M.; Muhammad, G.; Hossain, M.S.; Amin, S.U. Cognitive IoT-Cloud Integration for Smart Healthcare: Case Study for Epileptic Seizure Detection and Monitoring. *Mob. Netw. Appl.* **2018**, *23*, 1624–1635. [[CrossRef](#)]
146. Ganesan, M.; Sivakumar, N. IoT based heart disease prediction and diagnosis model for healthcare using machine learning models. In Proceedings of the 2019 IEEE International Conference on System, Computation, Automation and Networking, ICSCAN 2019, Pondicherry, India, 29–30 March 2019; pp. 1–5. [[CrossRef](#)]

147. Mohapatra, S.; Patra, P.K.; Mohanty, S.; Pati, B. Smart Health Care System using Data Mining. In Proceedings of the 2018 International Conference on Information Technology, ICIT 2018, Bhubaneswar, India, 19–21 December 2018; pp. 44–49. [\[CrossRef\]](#)
148. Kaur, P.; Kumar, R.; Kumar, M. A healthcare monitoring system using random forest and internet of things (IoT). *Multimed. Tools Appl.* **2019**, *78*, 19905–19916. [\[CrossRef\]](#)
149. Alhussein, M. Monitoring Parkinson’s Disease in Smart Cities. *IEEE Access* **2017**, *5*, 19835–19841. [\[CrossRef\]](#)
150. Tuli, S.; Basumatary, N.; Gill, S.S.; Kahani, M.; Arya, R.C.; Wander, G.S.; Buyya, R. HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. *Future Gener. Comput. Syst.* **2020**, *104*, 187–200. [\[CrossRef\]](#)
151. Devarajan, M.; Ravi, L. Intelligent cyber-physical system for an efficient detection of Parkinson disease using fog computing. *Multimed. Tools Appl.* **2019**, *78*, 32695–32719. [\[CrossRef\]](#)
152. Sayeed, M.A.; Mohanty, S.P.; Kougiannos, E.; Yanambaka, V.P.; Zaveri, H. A robust and fast seizure detector for IoT edge. In Proceedings of the 2018 IEEE 4th International Symposium on Smart Electronic Systems, iSES 2018, Hyderabad, India, 17–19 December 2018; pp. 156–160. [\[CrossRef\]](#)
153. Queralta, J.P.; Gia, T.N.; Tenhunen, H.; Westerlund, T. Edge-AI in LoRa-based health monitoring: Fall detection system with fog computing and LSTM recurrent neural networks. In Proceedings of the 2019 42nd international conference on telecommunications and signal processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 601–604.
154. Awais, M.; Raza, M.; Singh, N.; Bashir, K.; Manzoor, U.; ul Islam, S.; Rodrigues, J.J. LSTM based Emotion Detection using Physiological Signals: IoT framework for Healthcare and Distance Learning in COVID-19. *IEEE Internet Things J.* **2020**. [\[CrossRef\]](#)
155. Pirzada, P.; White, N.; Wilde, A. Sensors in smart homes for independent living of the elderly. In Proceedings of the 5th International Multi-Topic ICT Conference: Technologies For Future Generations, IMTIC 2018—Proceedings, Jamshoro, Pakistan, 25–27 April 2018; pp. 1–8. [\[CrossRef\]](#)
156. Park, J.; Jang, K.; Yang, S.B. Deep neural networks for activity recognition with multi-sensor data in a smart home. In Proceedings of the IEEE World Forum on Internet of Things, WF-IoT 2018—Proceedings, Singapore, 5–8 February 2018; , pp. 155–160. [\[CrossRef\]](#)
157. Wang, A.; Chen, G.; Shang, C.; Zhang, M.; Liu, L. Human activity recognition in a smart home environment with stacked denoising autoencoders. In Proceedings of the International Conference on Web-Age Information Management, Nanchang, China, 3–5 June 2016; pp. 29–40.
158. Singh, D.; Merdivan, E.; Psychoula, I.; Kropf, J.; Hanke, S.; Geist, M.; Holzinger, A. Human activity recognition using recurrent neural networks. *Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinform.)* **2017**, *10410 LNCS*, 267–274. [\[CrossRef\]](#)
159. Kim, G.Y.; Shin, S.S.; Kim, J.Y.; Kim, H.G. Haptic Conversion Using Detected Sound Event in Home Monitoring System for the Hard-of-Hearing. In Proceedings of the HAVE 2018—IEEE International Symposium on Haptic, Audio-Visual Environments and Games, Proceedings, Dalian, China, 20–21 September 2018; pp. 17–22. [\[CrossRef\]](#)
160. Adege, A.B.; Lin, H.P.; Tarekegn, G.B.; Jeng, S.S. Applying deep neural network (DNN) for robust indoor localization in multi-building environment. *Appl. Sci.* **2018**, *8*, 62. [\[CrossRef\]](#)
161. Adeogun, R.; Rodriguez, I.; Razzaghpour, M.; Berardinelli, G.; Christensen, P.H.; Mogensen, P.E. Indoor occupancy detection and estimation using machine learning and measurements from an IoT LoRa-based monitoring system. In Proceedings of the 2019 Global IoT Summit (GloTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–5.
162. Zimmermann, L.; Weigel, R.; Fischer, G. Fusion of nonintrusive environmental sensors for occupancy detection in smart homes. *IEEE Internet Things J.* **2018**, *5*, 2343–2352. [\[CrossRef\]](#)
163. Chowdhry, D.; Paranjape, R.; Laforge, P. Smart home automation system for intrusion detection. In Proceedings of the 2015 IEEE 14th Canadian Workshop on Information Theory, CWIT 2015, St. John’s, NL, Canada, 6–9 July 2015; pp. 75–78. [\[CrossRef\]](#)
164. Bhide, V.H.; Wagh, S. I-learning IoT: An intelligent self learning system for home automation using IoT. In Proceedings of the 2015 International Conference on Communication and Signal Processing, ICCSP 2015, Melmaruvathur, India, 2–4 April 2015; pp. 1763–1767. [\[CrossRef\]](#)
165. Garcia, F.C.C.; Creayla, C.M.C.; Macabebe, E.Q.B. Development of an Intelligent System for Smart Home Energy Disaggregation Using Stacked Denoising Autoencoders. *Procedia Comput. Sci.* **2017**, *105*, 248–255. [\[CrossRef\]](#)
166. Yang, C.C.; Soh, C.S.; Yap, V.V. A non-intrusive appliance load monitoring for efficient energy consumption based on Naive Bayes classifier. *Sustain. Comput. Inf. Syst.* **2017**, *14*, 34–42. [\[CrossRef\]](#)
167. Popa, D.; Pop, F.; Serbanescu, C.; Castiglione, A. Deep learning model for home automation and energy reduction in a smart home environment platform. *Neural Comput. Appl.* **2019**, *31*, 1317–1337. [\[CrossRef\]](#)
168. Konstantakopoulos, I.C.; Barkan, A.R.; He, S.; Veeravalli, T.; Liu, H.; Spanos, C. A deep learning and gamification approach to improving human-building interaction and energy efficiency in smart infrastructure. *Appl. Energy* **2019**, *237*, 810–821. [\[CrossRef\]](#)
169. Albataineh, H.; Nijim, M.; Bollampall, D. The Design of a Novel Smart Home Control System using Smart Grid Based on Edge and Cloud Computing. In Proceedings of the 2020 IEEE 8th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–14 August 2020; pp. 88–91.
170. Sousa, P.H.F.; Nascimento, N.M.M.; Almeida, J.S.; Rebouças Filho, P.P.; Albuquerque, V.H.C. Intelligent Incipient Fault Detection in Wind Turbines based on Industrial IoT Environment. *J. Artif. Intell. Syst.* **2019**, *1*, 1. [\[CrossRef\]](#)

171. Salhaoui, M.; Guerrero-González, A.; Arioua, M.; Ortiz, F.J.; El Oualkadi, A.; Torregrosa, C.L. Smart industrial iot monitoring and control system based on UAV and cloud computing applied to a concrete plant. *Sensors* **2019**, *19*, 3316. [[CrossRef](#)] [[PubMed](#)]
172. Ferreira, M.A.; De Souza, L.F.F.; Dos Silva, F.H.S.; Ohata, E.F.; Almeida, J.S.; Filho, P.P. Intelligent Industrial IoT system for detection of short-circuit failure in windings of wind turbines. In Proceedings of the Proceedings of the International Joint Conference on Neural Networks, Glasgow, UK, 19–24 July 2020. [[CrossRef](#)]
173. Nkonyana, T.; Sun, Y.; Twala, B.; Dogo, E. Performance evaluation of data mining techniques in steel manufacturing industry. *Procedia Manuf.* **2019**, *35*, 623–628. [[CrossRef](#)]
174. Siegel, J.E.; Pratt, S.; Sun, Y.; Sarma, S.E. Real-time Deep Neural Networks for internet-enabled arc-fault detection. *Eng. Appl. Artif. Intell.* **2018**, *74*, 35–42. [[CrossRef](#)]
175. Windau, J.; Itti, L. Inertial Machine Monitoring System for Automated Failure Detection. In Proceedings of the IEEE International Conference on Robotics and Automation, Brisbane, Australia, 21–25 May 2018; pp. 93–98. [[CrossRef](#)]
176. Sokolov, A.N.; Pyatnitsky, I.A.; Alabugin, S.K. Research of Classical Machine Learning Methods and Deep Learning Models Effectiveness in Detecting Anomalies of Industrial Control System. In Proceedings of the 2018 Global Smart Industry Conference, GloSIC 2018, Chelyabinsk, Russia, 13–15 November 2018. [[CrossRef](#)]
177. Huang, D.C.; Lin, C.F.; Chen, C.Y.; Sze, J.R. The Internet technology for defect detection system with deep learning method in smart factory. In Proceedings of the 2018 4th International Conference on Information Management, ICIM 2018, Oxford, UK, 25–27 May 2018; pp. 98–102. [[CrossRef](#)]
178. Li, L.; Ota, K.; Dong, M. Deep Learning for Smart Industry: Efficient Manufacture Inspection System with Fog Computing. *IEEE Trans. Ind. Inf.* **2018**, *14*, 4665–4673. [[CrossRef](#)]
179. Lin, S.Y.; Du, Y.; Ko, P.C.; Wu, T.J.; Ho, P.T.; Sivakumar, V.; Subbareddy, R. Fog Computing Based Hybrid Deep Learning Framework in effective inspection system for smart manufacturing. *Comput. Commun.* **2020**, *160*, 636–642. [[CrossRef](#)]
180. Garmaroodi, M.S.S.; Farivar, F.; Haghighi, M.S.; Shoorehdeli, M.A.; Jolfaei, A. Detection of Anomalies in Industrial IoT Systems by Data Mining: Study of CHRIST Osmotron Water Purification System. *IEEE Internet Things J.* **2020**, *4662*, 1. [[CrossRef](#)]
181. Park, D.; Kim, S.; An, Y.; Jung, J.Y. Lired: A light-weight real-time fault detection system for edge computing using LSTM recurrent neural networks. *Sensors* **2018**, *18*, 2110. [[CrossRef](#)]
182. Liu, Y.; Kumar, N.; Xiong, Z.; Lim, W.Y.B.; Kang, J.; Niyato, D. Communication-Efficient Federated Learning for Anomaly Detection in Industrial Internet of Things. In Proceedings of the GLOBECOM, Taipei City, Taiwan, 7–10 December 2020; Volume 2020, pp. 1–6.
183. Zheng, H.; Feng, Y.; Gao, Y.; Tan, J. A robust predicted performance analysis approach for data-driven product development in the industrial internet of things. *Sensors* **2018**, *18*, 2871. [[CrossRef](#)]
184. Essien, A.; Giannetti, C. A Deep Learning Model for Smart Manufacturing Using Convolutional LSTM Neural Network Autoencoders. *IEEE Trans. Ind. Inf.* **2020**, *16*, 6069–6078. [[CrossRef](#)]
185. Tao, W.; Lai, Z.H.; Leu, M.C.; Yin, Z. Worker Activity Recognition in Smart Manufacturing Using IMU and sEMG Signals with Convolutional Neural Networks. *Procedia Manuf.* **2018**, *26*, 1159–1166. [[CrossRef](#)]
186. Forkan, A.R.M.; Montori, F.; Georgakopoulos, D.; Jayaraman, P.P.; Yavari, A.; Morshed, A. An industrial IoT solution for evaluating workers' performance via activity recognition. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1393–1403.
187. Huang, B.; Wang, W.; Ren, S.; Zhong, R.Y.; Jiang, J. A proactive task dispatching method based on future bottleneck prediction for the smart factory. *Int. J. Comput. Integr. Manuf.* **2019**, *32*, 278–293. [[CrossRef](#)]
188. Brik, B.; Bettayeb, B.; Sahnoun, M.; Duval, F. Towards predicting system disruption in industry 4.0: Machine learning-based approach. *Procedia Comput. Sci.* **2019**, *151*, 667–674. [[CrossRef](#)]
189. Han, Y.; Zhang, C.J.; Wang, L.; Zhang, Y.C. Industrial IoT for Intelligent Steelmaking with Converter Mouth Flame Spectrum Information Processed by Deep Learning. *IEEE Trans. Ind. Inf.* **2020**, *16*, 2640–2650. [[CrossRef](#)]
190. Wang, T.; Wang, X.; Ma, R.; Li, X.; Hu, X.; Chan, F.T.; Ruan, J. Random Forest-Bayesian Optimization for Product Quality Prediction with Large-Scale Dimensions in Process Industrial Cyber-Physical Systems. *IEEE Internet Things J.* **2020**, *7*, 8641–8653. [[CrossRef](#)]
191. Spendla, L.; Kebisek, M.; Tanuska, P.; Hrcka, L. Concept of predictive maintenance of production systems in accordance with industry 4.0. In Proceedings of the 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMII), Herl'any, Slovakia, 26–28 January 2017; pp. 405–410.
192. Hwang, S.; Jeong, J.; Kang, Y. SVM-RBM based predictive maintenance scheme for IoT-enabled smart factory. In Proceedings of the 2018 13th International Conference on Digital Information Management, ICDIM 2018, Berlin, Germany, 24–26 September 2018; pp. 162–167. [[CrossRef](#)]
193. Jung-Hyok Kwon, E.J.K. Failure Prediction Model Using Iterative Feature Selection for Industrial Internet of Things. *Symmetry* **2019**, *12*, 454. [[CrossRef](#)]
194. Zhang, W.; Guo, W.; Liu, X.; Liu, Y.; Zhou, J.; Li, B.; Lu, Q.; Yang, S. LSTM-Based Analysis of Industrial IoT Equipment. *IEEE Access* **2018**, *6*, 23551–23560. [[CrossRef](#)]
195. Diez, A.; Khoa, N.L.D.; Makki Alamdari, M.; Wang, Y.; Chen, F.; Runcie, P. A clustering approach for structural health monitoring on bridges. *J. Civ. Struct. Health Monit.* **2016**, *6*, 429–445. [[CrossRef](#)]

196. Guo, J.; Xie, X.; Bie, R.; Sun, L. Structural health monitoring by using a sparse coding-based deep learning algorithm with wireless sensor networks. *Pers. Ubiquitous Comput.* **2014**, *18*, 1977–1987. [[CrossRef](#)]
197. Gui, G.; Pan, H.; Lin, Z.; Li, Y.; Yuan, Z. Data-driven support vector machine with optimization techniques for structural health monitoring and damage detection. *KSCE J. Civ. Eng.* **2017**, *21*, 523–534. [[CrossRef](#)]
198. Dang, H.V.; Tran-Ngoc, H.; Nguyen, T.V.; Bui-Tien, T.; De Roeck, G.; Nguyen, H.X. Data-driven structural health monitoring using feature fusion and hybrid deep learning. *IEEE Trans. Autom. Sci. Eng.* **2020**. [[CrossRef](#)]
199. Vitola, J.; Pozo, F.; Tibaduiza, D.A.; Anaya, M. A sensor data fusion system based on k-nearest neighbor pattern classification for structural health monitoring applications. *Sensors* **2017**, *17*, 417. [[CrossRef](#)] [[PubMed](#)]
200. Yu, J.; Kim, M.; Bang, H.C.; Bae, S.H.; Kim, S.J. IoT as applications: cloud-based building management systems for the internet of things. *Multimed. Tools Appl.* **2016**, *75*, 14583–14596. [[CrossRef](#)]
201. Singaravel, S.; Geyer, P.; Suykens, J. Deep neural network architectures for component-based machine learning model in building energy predictions. In Proceedings of the Digital Proceedings of the 24th EG-ICE International Workshop on Intelligent Computing in Engineering, Nottingham, UK, 10–12 July 2017.
202. Eltresy, N.A.; Dardeer, O.M.; Al-Habal, A.; Elhariri, E.; Hassan, A.H.; Khattab, A.; Elsheakh, D.N.; Taie, S.A.; Mostafa, H.; Elsadek, H.A.; et al. RF energy harvesting IoT system for museum ambience control with deep learning. *Sensors* **2019**, *19*, 4465. [[CrossRef](#)] [[PubMed](#)]
203. Hu, W.; Wen, Y.; Guan, K.; Jin, G.; Tseng, K.J. itcm: Toward learning-based thermal comfort modeling via pervasive sensing for smart buildings. *IEEE Internet Things J.* **2018**, *5*, 4164–4177. [[CrossRef](#)]
204. Ferrández-Pastor, F.J.; Mora, H.; Jimeno-Morenilla, A.; Volckaert, B. Deployment of IoT edge and fog computing technologies to develop smart building services. *Sustainability* **2018**, *10*, 3832. [[CrossRef](#)]
205. Stolfi, D.H.; Alba, E.; Yao, X. Predicting car park occupancy rates in smart cities. In Proceedings of the International Conference on Smart Cities, Malaga, Spain, 14–16 June 2017; pp. 107–117. [[CrossRef](#)]
206. Lenka, R.K.; Barik, R.K.; Das, N.K.; Agarwal, K.; Mohanty, D.; Vipsita, S. PSPS: An IoT based predictive smart parking system. In Proceedings of the 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics, UPCON 2017, Mathura, India, 26–28 October 2017; pp. 311–317. [[CrossRef](#)]
207. Ali, G.; Ali, T.; Irfan, M.; Draz, U.; Sohail, M.; Glowacz, A.; Sulowicz, M.; Mielnik, R.; Faheem, Z.B.; Martis, C. IoT Based Smart Parking System Using Deep Long Short Memory Network. *Electronics* **2020**, *9*, 1696. [[CrossRef](#)]
208. Ebuchi, T.; Yamamoto, H. Vehicle/pedestrian localization system using multiple radio beacons and machine learning for smart parking. In Proceedings of the 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC), Okinawa, Japan, 11–13 February 2019; pp. 086–091.
209. Awan, F.M.; Saleem, Y.; Minerva, R.; Crespi, N. A comparative analysis of machine/deep learning models for parking space availability prediction. *Sensors* **2020**, *20*, 322. [[CrossRef](#)]
210. Sevillano, X.; Märmol, E.; Fernandez-Arguedas, V. Towards smart traffic management systems: Vacant on-street parking spot detection based on video analytics. In Proceedings of the FUSION 2014—17th International Conference on Information Fusion, Salamanca, Spain, 7–10 July 2014.
211. Bura, H.; Lin, N.; Kumar, N.; Malekar, S.; Nagaraj, S.; Liu, K. An edge based smart parking solution using camera networks and deep learning. In Proceedings of the 2018 IEEE International Conference on Cognitive Computing (ICCC), San Francisco, CA, USA, 2–7 July 2018; pp. 17–24.
212. Lee, C.; Park, S.; Yang, T.; Lee, S.H. Smart parking with fine-grained localization and user status sensing based on edge computing. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–5.
213. Aung, S.S.; Naing, T.T. Naïve Bayes Classifier Based Traffic Prediction System on Cloud Infrastructure. In Proceedings of the International Conference on Intelligent Systems, Modelling and Simulation, ISMS, Kuala Lumpur, Malaysia, 9–12 February 2015; pp. 193–198. [[CrossRef](#)]
214. Liu, Y.; Wu, H. Prediction of road traffic congestion based on random forest. In Proceedings of the 2017 10th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China, 9–10 December 2017; Volume 2, pp. 361–364.
215. Wei, W.; Wu, H.; Ma, H. An autoencoder and LSTM-based traffic flow prediction method. *Sensors* **2019**, *19*, 2946. [[CrossRef](#)] [[PubMed](#)]
216. Xiao, Y.; Yin, Y. Hybrid LSTM neural network for short-term traffic flow prediction. *Information* **2019**, *10*, 105. [[CrossRef](#)]
217. Sun, F.; Pan, Y.; White, J.; Dubey, A. Real-Time and Predictive Analytics for Smart Public Transportation Decision Support System. In Proceedings of the 2016 IEEE International Conference on Smart Computing, SMARTCOMP 2016, St Louis, MO, USA, 18–20 May 2016; pp. 1–8. [[CrossRef](#)]
218. Dogru, N.; Subasi, A. Traffic accident detection using random forest classifier. In Proceedings of the 2018 15th Learning and Technology Conference, L and T 2018, Jeddah, Saudi Arabia, 25–26 February 2018; pp. 40–45. [[CrossRef](#)]
219. Nallaperuma, D.; Nawaratne, R.; Bandaragoda, T.; Adikari, A.; Nguyen, S. Online Incremental Machine Learning Platform for Big Data-Driven Smart Traffic Management. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 4679–4690. [[CrossRef](#)]
220. Mukherji, A.; Raghuram, V.; Pandey, S.; Tran, H.; Bulusu, N. CommuterScanner: Towards Smart Indoor Positioning Systems in Urban Transportation. In Proceedings of the 2019 11th International Conference on Communication Systems & Networks (COMSNETS), Bangalore, India, 7–11 January 2019; pp. 619–624.

221. Majumdar, S.; Subhani, M.M.; Roullier, B.; Anjum, A.; Zhu, R. Congestion prediction for smart sustainable cities using IoT and machine learning approaches. *Sustain. Cities Soc.* **2021**, *64*, 102500. [[CrossRef](#)]
222. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [[CrossRef](#)]
223. Braun, T.; Fung, B.C.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [[CrossRef](#)]
224. Eckhoff, D.; Wagner, I. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 489–516. [[CrossRef](#)]
225. Elmaghraby, A.S.; Losavio, M.M. Cyber security challenges in smart cities: Safety, security and privacy. *J. Adv. Res.* **2014**, *5*, 491–497. [[CrossRef](#)] [[PubMed](#)]
226. POPESCUL, D.; RADU, L.D. Data Security in Smart Cities: Challenges and Solutions. *Inform. Econ.* **2016**, *20*, 29–38. [[CrossRef](#)]
227. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [[CrossRef](#)]
228. Whitehead, D.E.; Owens, K.; Gammel, D.; Smith, J. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In Proceedings of the 70th Annual Conference for Protective Relay Engineers, CPRE 2017, College Station, TX, USA, 3–6 April 2017. [[CrossRef](#)]
229. Ang, I.B.A.; Salim, F.D.; Hamilton, M. Human occupancy recognition with multivariate ambient sensors. In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), Sydney, Australia, 14–18 March 2016; pp. 1–6.
230. Yang, L.; Ting, K.; Srivastava, M.B. Inferring occupancy from opportunistically available sensor data. In Proceedings of the 2014 IEEE International Conference on Pervasive Computing and Communications, PerCom 2014, Budapest, Hungary, 24–28 March 2014; pp. 60–68. [[CrossRef](#)]
231. Howard, J.D.; Longstaff, T.A. *A Common Language for Computer Security Incidents*; Technical Report; Sandia National Labs: Albuquerque, NM, USA, 1998.
232. Agrawal, R.; Verma, P.; Sonanis, R.; Goel, U.; De, A.; Kondaveeti, S.A.; Shekhar, S. Continuous security in IoT using blockchain. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing—Proceedings, Calgary, AB, Canada, 15–20 April 2018; pp. 6423–6427. [[CrossRef](#)]
233. Rizvi, S.; Iii, J.P.; Kurtz, A.; Rizvi, M. Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing Furthermore, Communications/12th IEEE International Conference On Big Data Science Furthermore, Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 163–168. [[CrossRef](#)]
234. Aldairi, A.; Tawalbeh, L. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Comput. Sci.* **2017**, *109*, 1086–1091. [[CrossRef](#)]
235. Ali, M.; Abrishamchi, N.; Abdullah, A.H.; Cheok, A.D.; Bielawski, K.S. Side Channel Attacks on Smart Home Systems: A Short Overview. In Proceedings of the IECON 2017—43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 29 October–1 November 2017; pp. 8144–8149.
236. Choi, J.; Kim, Y. An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system. In Proceedings of the 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA). Asia Pacific Signal and Information Processing Association, Jeju, Korea, 13–16 December 2016; pp. 1–4. [[CrossRef](#)]
237. Al-Garadi, M.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *arXiv* **2018**, arXiv:1807.11023.
238. Ouyang, X.; Ma, Z. Using LSTM networks to identify false data of smart terminals in the smart grid. In Proceedings of the Proceedings of the International Conference on Parallel and Distributed Systems—ICPADS, Shenzhen, China, 15–17 December 2017; pp. 765–768. [[CrossRef](#)]
239. Diro, A.; Chilamkurti, N. Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications. *IEEE Commun. Mag.* **2018**, *56*, 124–130. [[CrossRef](#)]
240. Balakrishnan, N.; Rajendran, A.; Pelusi, D.; Ponnusamy, V. Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. *Internet Things* **2019**, 100112. [[CrossRef](#)]
241. Khatoun, R.; Zeadally, S. Cybersecurity and privacy solutions in smart cities. *IEEE Commun. Mag.* **2017**, *55*, 51–59. [[CrossRef](#)]
242. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G. Blockchain with internet of things: Benefits, challenges, and future directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40–48. [[CrossRef](#)]