



An Extended Review on Internet of Things (IoT) and its Promising Applications

Yusuf Perwej
Assistant Professor
Dept. of Information Technology
Al Baha University, Al Baha
Kingdom of Saudi Arabia

Bedine Kerim
Assistant Professor
Dept. of Information Technology
Al Baha University, Al Baha
Kingdom of Saudi Arabia

Mahmoud Ahmed AbouGhaly
Assistant Professor
Dept. of Information Technology
Al Baha University, Al Baha
Kingdom of Saudi Arabia

Hani Ali Mahmoud Harb
Assistant Professor
Dept. of Computer Engineering
Al Baha University, Al Baha
Kingdom of Saudi Arabia

ABSTRACT

At present IoT is immensely a descriptive term of a vision that everything should be connected to the internet. IoT applications have been widely used in several fields of social living such as healthcare and social products, industrial automation and energy. In this scenario, there are more than 14 billion interconnected digital and electronic devices in operation worldwide, the equivalent of almost two devices for every human being on earth. The IoT connects different non-living objects through the internet and enables them to share information with their community network to automate processes for human beings and makes their lives convenient. Subsequently, objects are being amalgamated with internet connectivity and powerful data analysis capabilities that promise to change the way we work and live. The Internet is a worldwide system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users globally. The most vital characteristics of IoT include connectivity, active engagement, connectivity, sensors, artificial intelligence, and small device use. This paper provides an overview of existing Internet of Things (IoT), technical details, and applications in this new emerging area as well as we are thoroughly analyzing the layer about the IoT. However, this manuscript will give a better understanding for the new researchers, who want to do research in this field of Internet of Things.

Keywords

Internet of Things (IoT), Data Lake, IoT Ecosystem, IoT Layer, Edge Computing, Things.

1. INTRODUCTION

Today the Internet has become ubiquitously, has touched almost every corner of the globe, and is affecting human life in implausible ways. We are now entering an era of even more comprehensive connectivity where a very wide variety of appliances will be connected to the web [1]. In general, the “Internet of Things” is the networking of physical objects connecting via the Internet. The Internet of Things is not a recently developed idea, as the devices have been communicating with each other for a number of years. The Internet of Things is an emerging topic of social, economic, and technical importance. The customer products, cars,

durable goods and trucks, industrial and utility components, sensors, and other daily objects are being combined with Internet connectivity and powerful data analytic proficiency that assurance to transform the way we work, live, and play [2]. This is becoming a famous concept across many vertical and horizontal markets, including a common man’s everyday life in the community, as it has several applications. The development of the Internet of Things [IoT] has been in the first instance driven by the needs of large corporations that stand to benefit greatly from the foresight and predictability afforded by the ability to follow all objects via the commodity chains in which they are embedded. For this intelligence and interconnection, [3] IoT devices are equipped with embedded actuators, processors, sensors, and transceivers. IoT is not a single technology; rather it is a heap of several technologies that work together in tandem. In the IoT actuators and sensors are devices, which help in interacting with the physical environment [4]. The data collected by the sensors have to be stored and processed intelligently in order to derive advantageous inferences from it. Presently, there are more than billions of interconnected digital and electronic devices in operation worldwide, the equivalent of nearly 2 devices for every human on earth. The Internet of Things finds several applications in entertainment, social life, health care, environment monitoring, home automation, fitness, education, transport systems, and energy conservation.

2. INTERNET OF THINGS (IoT)

The term “Internet of Things,” also known as “cyber–physical systems,” at the macro level, was first coined by Kevin Ashton in his presentation made to Procter & Gamble (P&G) in 1999 [3]. Kevin was working in MIT’s AutoID Lab to improve P&G business by linking its supply chain with Radio-Frequency Identification (RFID) information to the Internet. IEEE has defined it as follows [5] extensively speaking, the Internet of Things is a system consisting of networks of actuators, sensors, and smart objects whose purpose is to interconnect ‘all’ things, including day-to-day and industrial objects, in such a way as to make them intelligent, programmable, and more competent of interacting with humans and each other shown in figure 1. The number of connected things in the world will have a thirty fold

increase between 2009 and 2020, thus by 2020 there will be 28 billion things that are connected to the Internet [6]. A generic way of describing the IoT process was implied in Mark Weiser’s ubiquitous computing, and it is well exemplified in the National Institute of Standards and Technology (NIST) big data reference architecture [7]. The architecture is organized around two axes representing the two Big data value chains firstly the information (horizontal axis) and secondly the Information Technology (IT) (vertical axis). Along the information axis, the value is created by data collection, preparation and curation, analytics, visualization, and access [8]. The concept of IoT is not new. Because programmable Logic Controller (PLC) in 1970s is a micro-model of the IoT system that was widely used to control machines and processes within a factory. A PLC consists of output (example for digital or analog data), inputs (example for sensors, actuator, and off & on switches), CPU, and communication between components. The PLC systems were within a factory, not connected to the Internet and cloud. The IoT and big data store and retrieve data and programs over the Internet, or cloud computing, as an alternative your computer’s hard drive or a dedicated Network-Attached Storage (NAS). There is no unique definition available for IoT that is admissible by the world community of users. The optimal definition for the IoT would be “An open and comprehensive network of intelligent objects that have the capacity to auto organize, share information, data and resources, reacting and acting in the face of circumstance and transformation in the environment”. The Internet of Things has components that range in complexity, from simple identification tags to complex machine-to-machine communication, cameras and radio-frequency identification tagging of shipments in the supply chain are well-established examples [9].

The objects are becoming increasing with computing and communication powers competent of reproducing and supersede human contemplation and senses in the virtual world [10]. The IoT involves sensors in order to collect information. Sensors are already being used in daily life activities; however, most people may not realize it. In this context, smartphones contain different kind of sensors, such as accelerometers, cameras, and GPS receivers. Built-in sensors are nothing new in today’s society [11]. The Kevin Ashton said that IoT is beforehand happening, but we might not see it differentiate to smartphones which can both be seen and touched. There are various technologies involved in the Internet of Things, namely as near-field communications (NFC), machine-to-machine communication (M2M) radio-frequency identification (RFID), as well as actuator networks and wireless sensor [12] etc.

3. THE INTERNET OF THINGS (IoT) ARCHITECTURE

In this section, we briefly describe the overview of the IoT architecture. It can be classified as a collection of devices equipped with sensors, actuators, and processors that communicate with each other to serve a meaningful aim. The Internet of Things (IoT) at the beginning utilized current Internet infrastructure and existing technologies to transform stand-alone objects [13] into interconnected smart objects. IoT has the power to transform the way we interact with our belongings, and in an industry or enterprise, it can transform the way the businesses run. IoT architecture can also be called as a phenomenon driven model. In the IoT architecture diagram which shows the building blocks of an IoT system and how they are connected to collect, process and store data shown in figure 2 [14].

3.1. Things

A thing, in the reference of the Internet of things (IoT), is an entity or physical object that has a unique identifier, an embedded system and the capability to transfer data over a network and actuators that permit things to act (for instance, to open or close a door, to switch on or off the light, to increase or decrease engine rotation speed and more) [13]. This concept includes buildings, vehicles, production machinery, fridges, street lamps, rehabilitation equipment and everything else imaginable. The sensors are not in all cases physically attached to the things, sensors may necessitate monitoring, for instance, what happens in the closest environment to a thing.

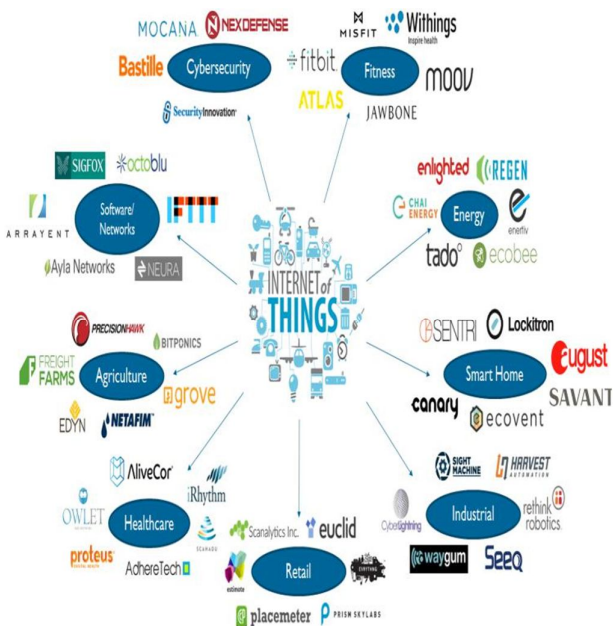


Fig 1: The Internet of Things (IoT)

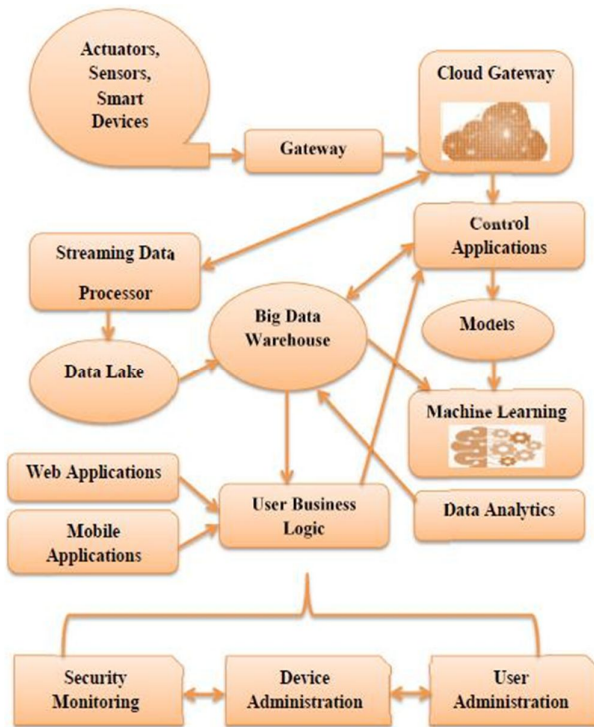


Fig 2: The Internet of Things (IoT) Architecture

3.2. Gateways

An Internet of Things (IoT) gateway is a software program or physical device that serves as the connection point between the cloud and controllers, sensors and intelligent devices shown in figure 3. Gateway is a translator, which permit two dissimilar protocols to communicate and routing the data to Cloud platform. Whole data motile to the cloud, or vice versa, go via the gateway, which can be either a dedicated hardware appliance or software program. An IoT gateway may also be referred to as an intelligent gateway or a handle tier. But when this network rise to hundreds & thousands of connected things or nodes, [15] preserve quality & reliability of the system is elementary task, in that scenario protocol requirement modification. These are low profile protocols in terms of bandwidth, battery powered, speed, having limited or zero ability to transfer the data to Cloud platform, since the network of connected objects is enormous, data generated by them are also enormous. Cloud gateway facilitates data compression and secure data transmission between field gateways and cloud IoT servers and also ensures compatibility with several protocols and communicates with field gateways using dissimilar protocols depending on what protocol is supported by gateways.

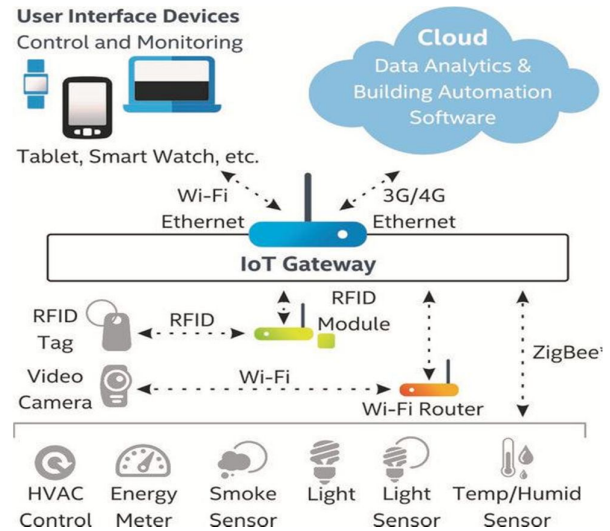


Fig 3: The Internet of Things (IoT) Gateways

3.3. Streaming Data Processor

When we add streaming capabilities to a piece of information infrastructures, we add the capability to automate real-time data flows. That is, we add the flexibility to ingest and process the increasing availability of IoT, social media, and other streaming data sources, and manage them alongside a conventional batch-based data. No data can be occasionally lost or useless.

3.4. Big Data Warehouse

A data warehouse is a database improves to analyze relational data coming from transactional systems and line of business applications. The data structure and schema are defined in advance to improve for fast SQL queries, where the outcome is typically used for operational reporting and analysis. Data is cleaned, enhance, and transformed so it can act as the single source of truth that users can faith. A big data warehouse holds only cleaned, matched and structured data. Also, data warehouse stores context knowledge about things and sensors and the commands, control applications send to things.

3.5. Data Lake

A data lake is a centralized repository that assent you to store all your structured and unstructured data at any scale shown in figure 4. You can store your data as is, without having to first structure the data, and run various types of analytics from dashboards and visualizations to big data processing, real-time analytics, and machine learning to guide superior decisions. Whereas the data is being expected for meaningful insights it's extracted from a data lake and loaded into a big data warehouse. A data lake is dissimilar, in view of the fact that it stores, relational data from line of business applications, and non-relational data from mobile apps, IoT devices, and social media [16]. The structure of the data or schema is not illuminated when data is apprehended. This means you can store all of your data without careful design or the requirement to know what questions you might need answers for in the future. The data lakes assent you to store relational data like operational databases and data from line of business applications, and non-relational data like mobile apps, social media, and IoT devices.

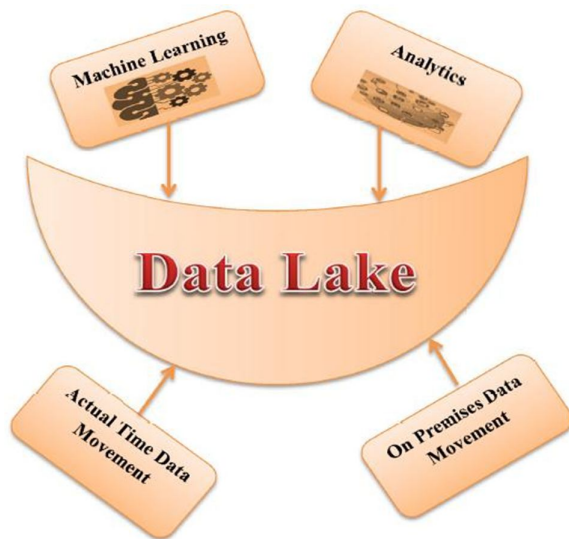


Fig 4: The Internet of Things (IoT) Data Lake

3.6. Data Analytics

The Internet of Things (IoT) is an interconnection of many devices, networks, technologies, and human resources to obtain a common goal. There are a diversified of IoT-based applications being used in various sectors and have succeeded in providing enormous benefits to the users. The data originate from IoT devices turns out to be of value only if it gets subjected to investigation, which brings data analytics into the picture. Data Analytics is defined as a process, which is used to check-up small and big data sets [1] with varying data properties to extract meaningful conclusions and actionable insights. These conclusions are usually in the form of patterns, trends, and statistics that aid business organizations in proactively engaging with data to implement effective decision-making processes [8] and also, the correlations and patterns found manually can further contribute to creating algorithms for control applications.

3.7. User Applications

The user applications are a software component of an IoT system which enables the connection of users to an IoT system and gives the options to monitor and control their smart things. Accompanied by a mobile or web app, users can monitor the state

of their things, set the options of automatic behavior, send commands to control applications.

3.8. Security Monitoring

The security is one of the most significant aspects of IoT. The IoT devices are often collecting highly personal data, and by their nature are bringing the real world onto the Internet. Connected things produce large volumes of data, which need to be securely transmitted and protected from cyber-criminals. The cyber-criminals can get the access to the “brain” of the whole IoT system and take control of it [17]. To stop such issue, it makes sense to log and analyze the commands sent by control applications to things, monitor the actions of users and store all these data in the cloud and it’s possible to cognize the patterns of suspicious behavior, store these samples and compare them with the logs generated by an IoT systems to

stop potential penetrations and reduce their influence on an IoT system.

3.9. Machine Learning

The machine learning, there is a chance to create more precise and more efficient models for control applications. Models are frequently updated based on the historical data accumulated in a big data warehouse. When the applicability and dexterity of new models are tested and approved by data analysts, new models are used by control applications. The commands sent by control apps to actuators can be also besides stored in a big data warehouse. This may help inquire into problematic cases. On the other aspect, storing commands from control apps may contribute to security, as an IoT system can identify that some commands are too comical or come in too big amounts which may evidence security breaches. The control applications can be either machine-learning based or rule-based. In the first, control apps are using models which are regularly updated with the historical data stored in a big data warehouse. In the second, control apps work as stated by to the rules stated by specialists. In spite of the fact that, control apps ensure superior automation of an IoT system, there should always be an option for users to impact the behavior of such applications.

3.10. User Management

User management is a contrivance which involves defining and handle users, roles and their access levels in a system. A typical user management implementation involves a wide range of functionality such as adding and removes users, controlling user activity via permissions, handle user roles, defining authentication policies, resetting user passwords etc.

3.11. Device Management

As many IoT deployments be composed of hundreds of thousands to millions of devices, it is necessary to track, monitor, and handle connected device fleets. In device management need to make sure your IoT devices work properly and securely after they have been deployed. In device management need to secure access to your devices, monitor health, detect and remotely troubleshoot issue, and manage software and firmware updates. IoT device management makes it convenient to securely on board, monitor, organize, and remotely handle IoT devices at scale. IoT device management, you can register your connected devices individually or in immensity, and effortlessly handle permissions so that devices remain secure. You can also organize your devices, query the state of any IoT device in your fleet, and send firmware updates over-the-air (OTA).

4. THE LAYER OF INTERNET OF THINGS (IoT)

In this section, we are discussing the IoT layer. IoT is managing millions of miscellaneous connected devices via the internet requires a flexible, layered architecture [18]. The IoT enabling technologies based on an extensive, common, and simple architecture, namely, the IoT five-layer model as depicted in figure 5 [19]. This model captures many of the essences of other models [20].

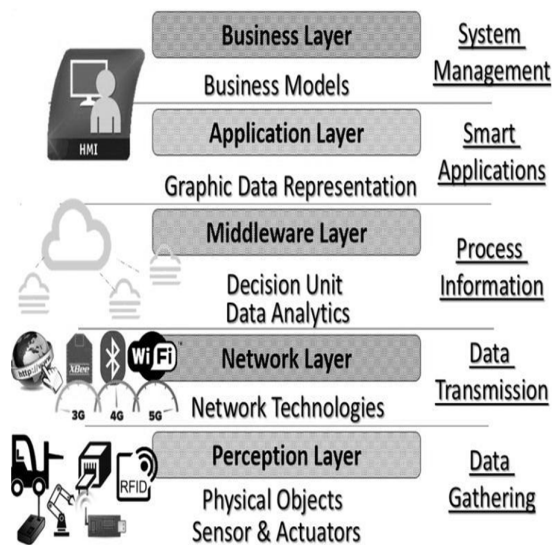


Fig 5: The Internet of Things (IoT) Layer

4.1. Perception Layer Technologies

The perception layer (also known as the objects layer) is the first layer (from the bottom, as shown in figure 5) in the IoT model. It contains several types of physical devices that are responsible for collecting data and acting in that manner, namely, temperatures, locations, object identifiers and humidity measurements. The power consumption and communication ability like unidirectional or bidirectional are significant aspects of this layer. The classification of the perception layer technologies is as follows.

4.1.1. Passive

Passive devices have the short radio coverage therefore they do not have on-board power supplies and rely on readers in close proximity for their energy supply. The restriction of passive enabling technologies is that communication with them is unidirectional. In this situation data can be read from nodes, but cannot be written back to the nodes. However, for many applications, unidirectional communication is enough.

4.1.2. Semipassive

In the semipassive devices have batteries that power tags while receiving signals from a reader. Dissimilar passive technologies, the extra obtainable power enable them to write and read data.

4.1.3. Active

In the active devices often have the extended range because they have larger batteries or are attached to power supplies that enable them to transmit and receive the data.

4.2. Network Layer Technologies

The network layer is the second layer. It is considered the infrastructure layer because its technologies transform the traditional sensors referred in the perception layer into smart and connected nodes. Network layer technologies enable nodes to be recognizable over the Internet or any local area network, which permits them to securely communicate with each other. The several technologies in this layer are also found in the first three layers in the IP suite (TCP/IP). Due to the conditioned capabilities of most IoT nodes, scalable and efficient routing techniques are needed to ensure

interoperability among IoT devices. Pay attention that many of IoT technologies are actually utilized in WSNs or machine to machine (M2M) communications but were ameliorate to meet IoT requirements. The several modern devices use more than one technology; as in smart watches, which often have Wi-Fi, Bluetooth, Li-Fi, and NFC [21] [22]. In this section, we classify the enabling technologies based on their functionality in the network layer.

4.2.1. Identification

When a node connects to the network, it is allocated a recognizer that enables it to communicate with other nodes. The identification is vital to control the excessive use of bandwidth in large by ensuring that only identified nodes communicate. To effortlessly locate devices in the massive network, names and addresses are allocated to the devices. The naming conventions allocate structured names to nodes, these names permit the nodes to be readily identified and may even specifically recognizer the functions.

4.2.2. Communication

Subsequently a node has been identified (for example named and addressed), it can start communicating with other nodes or with backend servers. In spite of that, this communication needs the selection of an appropriate communication medium, which depends on the capabilities of the node. Pay attention that can communicate horizontally or vertically.

4.2.3. Security

Due to a huge number of nodes with finite capabilities, security is an important and challenging task because a victorious attack is likely to cause excessive damage (for example Distributed Denial-of-Service attacks) [23]. The security may not be built into the different communication technologies. Consequently, additional security mechanisms must be provided by different layers to minimize the likelihood of attacks. Attacks can occur in this layer due to unsafe communication among nodes. Consequently, lightweight security mechanisms are needed for secure communication.

4.2.4. Routing

If a node knows a destination address, it must have an adept method for routing data to that destination node. The adept routing is critical in IoT environments because of the huge number of nodes that can be connected in an ad hoc manner. Due to the finite capabilities of IoT nodes, each node must efficiently learn about the best route. For that reason, a special routing protocol was introduced for these environments. Routing protocol for inferior power and lossy networks is an IPv6 routing standard protocol for resource finite devices [21]. This protocol was proposed to support dissimilar types of links, such as IEEE 802.15.4, and common traffic types, including many-to-one, one-to-many and one-to-one. The protocol can be dexterously represented as a set of graphs in which each graph is a Destination-Oriented Directed Acyclic Graph (DODAG). In this type of graph, each node is aware at least one path to its root node and each node is aware of its parent. The nodes exchange RPL particular messages to maintain the graph and make sure that a valid route to the root is always available.



4.3. Middleware Technologies

The middleware layer is the core of the IoT environment. It can be mapped to the application layer in the IP suite (TCP/IP). Technologies in this layer are frequently supported by IoT platforms. This layer enables services to be identified and requested based on names and addresses and enables programmers to communicate with miscellaneous objects, regardless of the specific hardware setup. This layer also processes received data, makes judgments, and delivers required services. The middleware layer execution those actions using the following technologies, which are divided into three groups based on their functionality.

4.3.1. Service Finding

In the IoT applications and user requirement to be able to use names or addresses to request services without knowledge the underlying infrastructure details. For that reason, services need to be registered and discoverable. Scalable and miscellaneous environments, service registration, and the quest should be autonomous, efficient, and dynamic.

4.3.2. Data Exchange

To handle the massive amount of data created by the huge number of nodes, a manager must transmit data to receivers in a secure and efficient manner. This management occurs on the TCP/IP application layer. Thus, the technologies that live in here are known as application protocols. In IoT environments, every node can capture data, analyze data, and control other nodes. In spite of, before a node can begin communicating and exchanging data in the IoT network, it must be identified and registered as a part of the service network [24]. This operation is designated to as node subscription. A subscribing node must make a request to join a service network prior to it can acquire or publish service-related data from or to the network. If the node is subscribed to publishers, it will receive service-related data when they are published. This model is known as the publish & subscribe model. Another possible approach is called request & response in which a joined node always requests a service-related data explicitly and receives a response that contains the requested data. The publish & subscribe model is commonly superior for IoT scenarios that require the huge deployment of nodes that continuously exchange data.

4.3.3. Computation

The computation is needed to process the collected data and manage sensors. Computations in IoT environments can range from convenient to complicated operations. The convenient computations are concerned with handling the platform, such as service access lists that involve decryption & encryption. The complicated computations address the genuine data.

4.4. Application Layer Technologies

This layer is accountable for providing requested services to IoT users through a simple interface without knowing how service requests are processed in the underlying layers. The IoT users can access a service (for example, tracking and managing vehicles or reading or setting temperature conditions remotely) using many platforms (for example smart watches, laptops, and smartphones) through web portals or applications. This service varies based on the IoT scenario, but can be categorized into four main classes as described in the below.

4.4.1. Identity Concerned Services

The identity concerned services require an identifier that is embedded in a node and a reader device, namely an RFID device. Identity concerned services can be active or passive. These services are extremely essential in IoT applications because they keep track of devices in huge deployments. A package-tracking application is an instance of this type of service.

4.4.2. Information Concentricity Services

The concentricity services summarize the collected raw sensory measurements from several types of sensors and networks that must be processed and reported to the IoT application. Load distribution among smart grids is an instance of this type of service.

4.4.3. Collaborative Cognizant Services

The collaborative cognizant services are built on top of information concentricity services and are used to make decisions about the obtained data. This type of service can be found in smart manufacturing, smart homes, smart agriculture, and among other applications. For instance, in a security system, a smart home, and smart thermostats are employed together to ameliorate security and energy efficiency based on sharing data between them.

4.4.4. Universal Services

These are the most profitable services of the IoT because they advance collaborative aware services to the next level by offering complete access to everything at any time and from ubiquitously. Access and control can be instating using a smartphone, computer, or any smart device. Smart cities are instances of these types of services.

4.5. Business Layer Technologies

In this layer, disparate the application layer, service data and IoT environmental data, namely business models, graphs, and flowcharts, can be accessed. This access helps administrators in the design, monitoring, analysis, implementation, evaluation, and development of IoT systems because the output of each of the already mentioned layers is analyzed in this layer to make services better and protect user privacy. The technologies in this layer can be divided into two categories based on their functions example for Big Data analytics and semantics, as described in the below sections.

4.5.1. Big Data Analytics

In the IoT environments involve an immense number of sensors that collect massive amounts of data, resulting in extremely huge datasets like big data that may be computationally analyzed to extract knowledge, such as trends, associations, and patterns [1]. The generated big data continues to increase as the IoT collects extra data. In consequence, need special technologies that can address the ever increasing amount of data are required. The most efficient action plan for addressing continuously increasing data is to process them in actual time streaming [8]. Actual time processing enables up-to-date analytics that reflect recent modifications of the data and conserves storage. In this context, machine learning can also utilize Big data to make accurate predictions. Besides, parallel computing can be employed using some IoT nodes to process data in parallel with backend servers for superior performance and load balancing. This technologies aid in the generation of actual -time analytics from big data.

4.5.2. Semantics

Afterward data are captured by sensors; they can be analyzed to extract information. Information is crucial for enhancing services and obtaining useful outcome that cannot be discovered without examining all IoT environment data. In order to analyze data efficiently, it has to be well-formed using some semantics technologies. The numerous semantic XML-based technologies can be used for information extraction, resource finding and usage, and modeling.

4.5.3. Apache Flink

Apache Flink is a tool for supporting Hadoop project structures and processing actual time data. As a type of batch processor, Flink contends with the conventional MapReduce and new Spark options. An open-source platform that is conceptually very homogeneous to Apex. Despite that, it is older than the Apex, it has not been used often in real-life, IoT projects due to its lack of auto scaling and finite message delivery guarantees (QoS) [25]. Apache Flink is also compatible with Apache YARN and other Hadoop respective tools.

4.5.4. Apache Spark

It is a well-known open-source distributed processing technology that utilizes in-memory caching and features enhanced execution of preferable performance. Apache Spark supports batch processing, streaming analytics, graph databases, ad hoc queries, and machine learning [26]. Apache Spark points out that it can be many times quicker than MapReduce, in some circumstances. Although Spark has been employed in numerous IoT systems, it needs some extra effort to overcome some barrier, such as time delays in the actual time process. Spark is a very flexible technology since it supports streaming data and static and several programming languages.

5. THE INTERNET OF THINGS (IoT) ECOSYSTEM

The Internet of Things ecosystem contains all the components that enable governments, businesses, and consumers to connect to their IoT devices. The ecosystem contains gateways, analytics, data storage, remotes, dashboards, networks, and security. At present, the IoT ecosystem, all physical things is digitized with digital services and cyber connected, interacted, and functioned to one another and to their physical surroundings [27]. Applying IoT technology will make terrific economic and environmental impacts that affect universal citizens. The following subsections list what potential IoT applications in various sectors that contains consumer, government, and enterprise shown in figure 6 fit simultaneously in the IoT ecosystem.

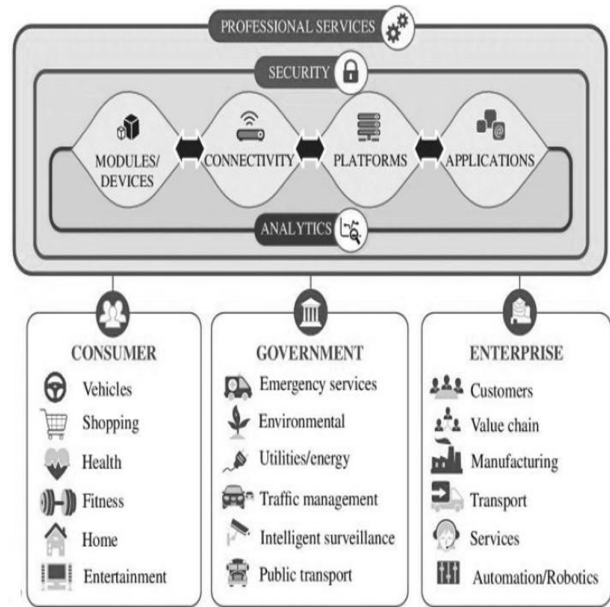


Fig 6: The Internet of Things (IoT) Ecosystem

Each subsection provides some examples that could be used to facilitate your thoughts to inspire and accelerate the pace of creativity, invention, and innovation. During the coming year over 25 billion devices expected to be installed by 2020 according to [28] Business Insider, the IoT ecosystem will touch almost every industry, including insurance, utilities, telecom, healthcare, smart homes, transportation, gas and oil and more. At first the consumer facing IoT applications contain smart home (example for home and chore automation, home robots, energy management, water management, safety and security, air quality), connected vehicles (example for logistics routing, operations management, autonomous vehicle, navigation, [27] condition-based maintenance), Healthcare contain (personal fitness illness monitoring and management, and wellness), and life and entertainment (example for gardening, hobby, water, music, and smart pet). Secondly the government facing IoT applications contain Smart city (example of parking meter, surveillance, power and lighting, adaptive traffic management, events control, natural or [28] human-made disaster management, emergency response system, resource management), smart transportation (example for connected car, roadway, fleet management, rail, aviation, port). In the smart grid (example of power line efficiency, demand response), smart water (example for domestic waterworks and waste water management), and environment (example for environmental monitoring, air quality, landfill and waste management). Thirdly the enterprise facing IoT applications contains energy (example for spill accident management, rigs and wells predictive maintenance, operating management), smart retails (example for self-checkout, in-store offers, digital signage, loss prevention, layout optimization, beacon routing, inventory control, [27] customer relationship management). In the smart banking (example for e-statement, online car, ATM machine, or home mortgage), smart building (example for education campus, stadium, office, hotel, airport, amusement park, fab and cleanroom, industrial building, data center), smart insurance (example for accident claims, natural disaster claims). In the smart logistics (example for shipment tracking,

real-time routing, connected navigation, flight navigation), and smart manufacturing (example for industrial automation, IIoTs, smart factory, robotics, asset management, energy management, operations management, predictive maintenance, and equipment optimization).

6. THE INTERNET OF THINGS (IoT) CLASSIFICATION

The Internet of Things (IoT) is an umbrella term which covering different distinctive base advances that went for connecting physical items and their virtual representation with the objective to use this connection for improve services and communication ideas [29]. The classification framework is based on an analysis of the produced scenarios. It manifest the specific features shared by the IoT scenarios which are needed to be considered to understand the scenarios superior, or one step ahead, to implement a scenario [30]. In the first and foremost architectural component of IoT is the perception layer. It collects data using sensors, which are the most essential drivers of the Internet of Things [31]. There are different types of sensors used in diverse IoT applications. The most common sensor available at present is the smartphone. The smartphone itself has several types of sensors embedded in it such as the camera, light sensor, microphone, proximity sensor, location sensor (GPS), movement sensors (accelerometer, gyroscope), and a magnetometer. These are being heavily used in various IoT applications. The numerous types of other sensors are beginning to be used such as sensors for pressure, humidity, measuring temperature, medical parameters of the body, chemical and neural signals, and biochemical substances. A class of sensors that stand out is infrared sensors that precede smartphones. In data preprocessing principally filter and summarize data before sending it on the network. This type of units typically has a small processing unit, a little amount of temporary storage, and some security features. The several communication technologies used for the Internet of Things. Several entities communicate over the network [30] using a diverse set of protocols and standards. The most general communication technologies for short range, low power communication protocols are NFC (Near Field Communication) and RFID (Radio Frequency Identification) [32]. For the medium range, they are Bluetooth [21], Zigbee, and WiFi, Li Fi [22]. Communication in the IoT world needed special networking protocols and mechanisms. Consequently, new mechanisms and protocols have been proposed and implemented for each layer of the networking stack, according to the necessity imposed by IoT devices. The middleware creates an abstraction for the programmer namely that the details of the hardware can be hidden. This renovates interoperability of smart things and makes it easy to offer various kinds of services [33]. In the applications of IoT focus on health and fitness, smart vehicular systems, home automation, ambient assisted living, smart cities, smart environments, smart grids, entertainment, and social life.

7. THE REFERENCE MODEL OF INTERNET OF THINGS (IoT)

The Internet of Things (IoT) is a worldwide industry movement that brings together process, data, people and things to make networked connections more pertinent and valuable than ever before. Nowadays, more than 99 percent of things in the world are not connected [34] and by 2020, it is estimated that 4.5 billion new people and 37 billion new

things will have joined the Internet. In the near the time to come, the growth and convergence of information, people, and things on the Internet will create unprecedented opportunity for countries, individuals, and industries. The IoT reference model does not conditioned the scope or locality of its components. The present IoT models confer levels of abstraction that are not aligned with the physical and logical network structure, nor do they capture the necessary details of diverse network architectures and protocols in use [35]. In our model, devices and physical links are at the lowest stage. His bottom layer consists of the physical topologies of a number of miscellaneous network technologies gateways to one-another directly, or to the Internet directly or via edge clouds [36]. In Figure 7 illustrates the IoT reference model and its stages. It is essential to note that in the IoT, data flows in both directions. In a control pattern, control information flows from the top of the model (stage7) to the bottom (stage1). In a monitoring pattern, the flow of information is the back up.

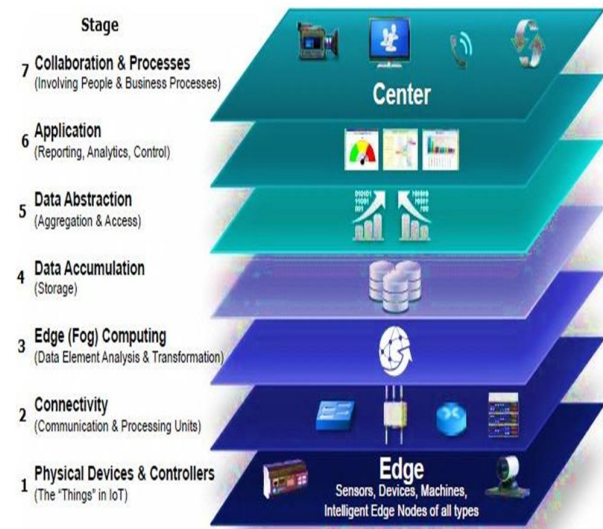


Fig 7: The Internet of Things (IoT) Reference Model

7.1. The Physical Devices and Controllers

The IoT reference model starts with physical devices and controllers that might control various devices. These are the “things” in the IoT, and they contain a wide range of endpoint devices that send and receive information. The devices are diverse, and there is no regulation about location, size, form factor, or beginning. Fewer devices will be the size of a silicon chip and few will be as huge as vehicles. The IoT must support the whole range.

7.2. The Connectivity

The connectivity is the most essential function of next stage is reliable, timely information transmission. The IoT reference model is for communications and processing to be carried out by existing networks. The IoT reference model does not need or indicate the creation of a various network it relies on existing networks. As first stage devices proliferate, the ways in which they interact with second stage connectivity equipment may modification. Unconcern of the details, first stage devices communicates through the IoT system by interacting with second stage connectivity equipment.

7.3. The Edge Computing



The miniature stage data processing at the gateway and sensor nodes is known as edge computing. The functions of third stage are driven by the need to convert network data flows into information that is appropriate for storage and higher stage processing at the fourth stage [37]. This means that third stage activities focus on high-volume data analysis and transformation. Given that data is generally submitted to the connectivity second stage networking equipment by devices in miniature units, third stage processing is performed on a packet-by-packet basis. This processing is finite, in view of the fact that, there is only understanding of data units not sessions or transactions.

7.4. The Data Accumulation

The data that is sent over the internet via gateways by the sensor nodes are obtained and stored in a database on the Cloud and the networking systems are built to dependably move data. Before to the fourth stage, data is moved via the network at the rate and organization determined by the devices produce the data. The event model is driven. As defined supra, first stage devices do not contain computing capabilities themselves [38]. Although, few computational activities could occur at the second stage, namely as protocol translation or application of network security policy. Additional compute tasks can be performed on the third stage, namely as packet inspection. The driving computational tasks as close to the edge of the IoT as possible, with miscellaneous systems, distributed across various management domains represents an example of fog computing. In the fourth stage converts event-based data to query-based processing. This is a deciding stage in bridging the differences between the world non-real-time application world and the real-time networking world.

7.5. The Data Abstraction

The primary purpose is to get the compulsory and significant data out of all the data that is collected. IoT systems will necessitate to scale to a corporate or even global level and will need several storage systems to accommodate IoT device data and data from conventional enterprise HRMS, CRM, ERP and other systems [39]. The data abstraction functions of fifth stage are focused on rendering data and its storage in ways that enable developing easy, performance-enhanced applications.

7.6. The Application

The analytics over the data and responding pursuant to the data to control the actuators at the sensor nodes is one of the primary applications of the IoT Architecture. The sixth stage is the application level, where information interpretation occurs. Software at this level interacts with fifth stage and data at rest, so it does not have to operate at network speeds. The IoT reference model does not rigidly define an application. The applications vary based on vertical markets, the nature of device data, and business requirement. Few applications will focus on monitoring device data. Few will focus on controlling devices and few combine device and non-device data. The monitoring and control applications delineate numerous various application models, application servers, hypervisors, multi-threading, multi-tenancy, programming patterns, and software stacks, leading to discussions of operating systems, mobility, etc.

7.7. The Collaboration and Processes

This is the seven stage of the IoT reference model. The human interaction and involvement in the IoT scenario are seen as the most neglected parts [40]. Not only the device should be smart sufficient to perform certain tasks, but they should also have some intuitive interactions with the human. One of the primary dissimilarity between the Internet of Things (IoT) and IoT is that IoT contain people and processes. This dissimilarity becomes particularly clear at seven stages. The IoT system, and the information it creates, is of little value unless it yields action, which frequently needs processes and people. Applications to perform business logic to empower people. People use applications and associated data for their specific necessity. Frequently, several people use the same application for a range of various purposes. So the objective is not the application it is to empower people to do their work superior. The people must be able to communicate and collaborate, sometimes using the conventional Internet, to make the IoT advantageous.

8. THE INTERNET OF THINGS (IoT) TECHNOLOGIES

The IoT primarily exploits networking technologies and standard protocols. However, the most important enabling technologies and protocols of IoT [41] are RFID, NFC, ZigBee, Bluetooth, Electronic Product Code (EPC), low-energy wireless, Barcode, LTE-A, Artificial Intelligence (AI), Wireless Sensor Networks (WSN), and WiFi-Direct [42]. These technologies support the particular networking functionality needed in an IoT system, in contrast to a standard uniform network of common systems [41]. The IoT enabled users to bring physical objects into the sphere of cyber world. This was made possible by various tagging technologies like RFID, NFC, and 2D barcode which permits physical objects to be identified and referred over the internet [43]. The IoT, which is integrated with radio frequency technology and sensor technology, is the omnipresent network based on the ubiquitously hardware resources on the internet, is the internet content objects together. It include, in addition to intricate technologies of computer and communication network outside [44], still contain many new auxiliary technologies of Internet of Things, namely collecting information technology, controlling technology, remote communication technology, remote information transmission technology, sea measures information intelligence analyzes and remote information transmission technology etc.

8.1. Radio Frequency Identification (RFID)

The RFID is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, person. A tag can be read from up to many feet away and does not require to be within direct line-of-sight of the reader to be tracked [45]. RFID technology plays an essential role in IoT find a solution to the identification dispute of objects around us in a cost effective manner [28]. The technology is classified into three categories based on the technique of power supply provision in Tags Active RFID, Semi Passive RFID and Passive RFID. The primary components of RFID are tagged, antenna, access controller, reader, software and server. It is more authentic, efficient, secured, cheap and accurate. This device can be sophisticated or simple, but it's not the device that matters it is the chip. The chip is so powerful that it can carry about 2,000



bytes of data that we can use to preferable our work, productivity, and lives.

8.2. Electronic Product Code (EPC)

The Electronic Product Code (EPC) is a distinctive number that identifies a specific item in the supply chain. The EPC can be allied with dynamic data, namely the origination point of an item or the date of its production [46]. Much like a Vehicle Identification Number (VIN) or Global Trade Item Number (GTIN), the EPC is key to unravel the power of the information systems that are part of the EPC global Network. The Electronic Product Code (EPC) is a 64 bit or 98 bit code electronically recorded on an RFID tag and plans to design a reformation in the EPC barcode system. EPC code can store information about the type of EPC, a distinctive serial number of products, its specifications, manufacturer information etc.

8.3. Low-Energy Wireless

This technology substitutes the most power hungry aspect of an IoT system. However, sensors and other elements can power down over long periods, communication links must stay in listening mode [47]. In the Low-energy wireless not only decrease consumption, but also extends the life of the device via lower use.

8.4. Barcode

A barcode, be made up of bars and spaces, is a machine-readable representation of numerals and characters. Today, packages of products sold at supermarkets, convenience stores and other stores are all over the place. These are barcodes [48]. There are 3 types of barcodes of 2 dimensional, Numeric and Alpha Numeric. The barcodes are designed to be machine readable and that can be read with an optical barcode scanner, they can also be read using a camera.

8.5. Wireless Fidelity (Wi-Fi)

Wi-Fi is a type of wireless network technology used for connecting to the Internet. The frequencies Wi-Fi works at are 2.4GHz or 5GHz, make sure no interference with TV antenna, broadcast radio, cellphones and two-way radios are encountered during transmission [49]. Wi-Fi is mainly just radio waves broadcast from a Wi-Fi router, a device detecting and deciphering the waves, and then sending back data to the router. It works very likewise for an FM & AM radio, but it is a two-way communication channel. Wi-Fi works over extended distances than Bluetooth or infrared and is also a low power unobtrusive technology, making it appropriate for portable devices such as laptops and palmtops. This technology include any type of WLAN product support any of the IEEE 802.11 together with dual-band, 802.11a, 802.11b, 802.11g and 802.11n.

8.6. LTE-A

LTE-A stands for LTE-advanced incorporated a number of new techniques that enabled the system to confer very much higher data rates, and also much excellent performance, especially at cell edges and other areas where performance would not normally have been so healthy [50]. LTE-A, delivers an essential upgrade to LTE technology by elongate, not only its coverage, but also deficiency its latency and raising its throughput. It gives IoT a terrific power via expanding its range, with its most valued applications being vehicle, UAV, and identical communication. The OFDM and MIMO are two of the fundamental technologies that will be enablers. LTE D2D is a provision that has been requested by a

number of users, in special the emergency services. It enables fast, intense access via direct communication. Accordingly LTE-advanced has provided refinement to both users and operators, as well as those endue additional services.

8.7. Bluetooth

Bluetooth is a short-range wireless communication technology that permits devices, namely computers, mobile phones, and peripherals to transmit data or voice wirelessly over a short distance. The aim of Bluetooth is to substitute the cables that normally connect devices, while still keeping the communications between them secure [21]. The "Bluetooth" name is taken from a 10th-century Danish king named Harald Bluetooth, who was said to unite disparate, warring regional factions. Bluetooth technology brings together a broad range of devices across many various industries via a unifying communication standard. A set of Bluetooth device sharing a common channel for communication is called Piconet. This Piconet is capable of 2 - 8 devices at a time for data sharing, and that data may be pictures, video, text, and sound [21]. The Bluetooth Special Interest Group comprises more than 1000 companies with HP, Aruba, Intel, Intel, Cisco, Ericson, IBM, Motorola and Toshiba. Bluetooth v3.0 + HS. Bluetooth high-speed technology devices can deliver up to 24 Mbps of data, which is faster than the 802.11b WiFi standard, but slower than wireless-a or wireless-g standards [47].

8.8. ZigBee

The Zigbee is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine and internet of things networks. ZigBee operates on the IEEE 802.15.4 specification and is used to create networks that need a low data transfer rate, secure networking and energy efficiency [51]. It is employed in a number of applications such as heating and cooling control, building automation systems, heating and cooling control and in medical devices. ZigBee has range of around 100 meters and a bandwidth of 250 kbps and the topologies that its works are star, cluster tree and mesh. ZigBee is designed to be easier and less costly than the other person is networked technologies like as Bluetooth.

8.9. Near Filed Communication (NFC)

Near Field Communication (NFC) is a set of short-range wireless technology at 13.56 MHz, typically be in need of a distance of 4 cm [52]. Near-field communication is a wireless technology that permits users to make payments by placing a compatible device like a smartphone or payment card within a few centimeters of another compatible device like a terminal, tablet or another smartphone. NFC tags are passive devices. They store data that can be repossessed by active NFC devices. Near-field communication transmits data via electromagnetic radio fields and is the technology behind payment services like Apple Pay and Google Wallet. This device must include NFC chips for an NFC transaction to take place. It also works in a dirty environment, does not need line of sight, easy and unpretentious connection method.

8.10. Wireless Sensor Networks (WSN) A

wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The normally monitored parameters are illumination intensity, vibration



intensity, sound intensity, temperature, humidity, pressure, wind direction and speed, power-line voltage, chemical concentrations, pollutant levels and vital body functions [53]. A wireless sensor network is an essential element in IoT paradigm. Sensor nodes may not have a global ID owing to the fact that of the huge amount of overhead and huge number of sensors. The WSN based on IoT has received noticeable attention in many areas, like as precision agriculture monitoring, manufacturing, homeland security, healthcare, habitat monitoring, forest fire, flood detection, and military etc [54].

8.11. Artificial Intelligence (AI)

Artificial Intelligence refers to electronic environments that are sensitive and responsible for the presence of people. In a comprehensive, intelligence world, devices work in concert to support people in carrying out their everyday life activities in convenient [55], natural way using information and intelligence that is hidden in the network connected devices [56]. It is distinguished by the following systems of characteristics first many networked devices are integrated into the environment, second devices can be aware you and your situational context, third they can be tailored to your necessity, fourth they can transform in response to you, fifth they can be prepared for your desires without conscious mediation.

8.12. Wi-Fi-Direct

Wi-Fi, Direct permission two devices establish a direct, peer-to-peer Wi-Fi connection without need a wireless router. The Wi-Fi becomes a way of communicating wirelessly like Bluetooth, but with less latency [57]. Wi-Fi-Direct removes an element of a network that frequently bogs it down, and it does not reconciliation on speed or throughput. The Wi-Fi, Direct is analogous in concept to “ad-hoc” Wi-Fi mode. However, unlike an ad-hoc Wi-Fi connection, Wi-Fi, Direct contain an effortless way to automatically explore nearby devices and connect to them. Wi-Fi, Direct is based on the IEEE 802.11 family of standards for wireless local area network (WLAN) operation. Wi-Fi, Direct devices uses WPA2 encryption, which is the most secure way of encrypting Wi-Fi.

9. APPLICATIONS OF INTERNET OF THINGS (IoT)

The Yarn schedulers are the proficient algorithms written to manage cluster resources. The Yarn resource manager service has a pluggable and authentic scheduler component, it does not observe or track the applications running in the cluster. It is answerable only for allocation of resources to executing applications. The scheduling in [17] Yarn is a pluggable framework to allocate cluster resources in a lot of the user environment. Be conditional on the use case and user requirement, administrators may prefer either a simple FIFO scheduler, capacity scheduler, or fair scheduler [16]. Now, we are discussing about the all three scheduler.

9.1. IoT in Smart Home

The smart home distinctly stands out, ranking as a highest IoT application on all measured channels. More than 70,000 people are presently searching for the term “Smart Home” each month. The cost of owning a house is the primus expenditure in a home owner’s life. Smart Home products are assurance to save time, energy and money. This is not a surprise. The IoT Analytics company database for Smart

Home includes more than 200 companies and startups. Several companies are active in smart home than any other application in the field of IoT. The total amount of funding for Smart Home startups nowadays exceeds \$2.5bn. This list contains prominent startup names such as Nest or AlertMe as well as a number of multinational corporations like Belkin, Haier, or Philips.

9.2. IoT in Tier Air Pressure Detection

This is one of the most special applications of IoT, where in the technology can enucleate the air pressure in your car tiers and give you information on under-inflation. In this technology, the sensors are embedded on the tiers which detect drops in air pressures and instantly send out signals to take suitable actions. This technology is built with an intention to foster safer driving conditions, where most people can be cautioned of under-inflated tiers.

9.3. IoT in Wearable’s

The Wearable’s continue to exist a hot topic too among potential IoT applications and devices are installed with sensors and software’s which collect data and information about the users. This data is later pre-processed to extract necessary insights about user. The prerequisite from internet of things technology for wearable applications is to be highly energy efficient or ultra-low power and small sized. As customer awaits the release of Apple’s new smart watch in April 2015, there are plenty of other wearable innovations to be thrilled about like the Sony Smart B Trainer, the Myo gesture control, or LookSee bracelet.

9.4. IoT in Smart City

The smart city extends a wide miscellaneousness of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its prominence is fueled by the fact that many smart city solutions promise to decrease real pains of people living in cities these days. IoT will find a solution major issue faced by the people living in cities like pollution, traffic overcrowding and shortage of energy supplies etc. The products like cellular communication enabled Smart Belly junk will send alerts to municipal services when a bin needs to be evacuated. By installing sensors and using web applications, citizens can explore free available parking slots across the city. Also, the sensors can detect meter tampering problem, general malfunctions and any installation problem in the electricity system.

9.5. IoT in Smart Eye

Next, a device straight from the Iron Man movies! The smart eye technology is very homogeneous to Google’s most ambitious project the Glass. This technology is equipped with sensors and connectivity options from Wi-Fi to Bluetooth to provide promiscuous options and accessibility features right in front of your eye but without causing a distraction. You can open maps, surf the internet, read emails or messages, capture moments and do more with these futuristic glasses.

9.6. IoT in Smart Grids

The power grids of the future will not only be smart adequate, but also highly credible. The Smart grid concept is becoming very famous all over the world. A future smart grid assurance to use information about the behaviors of electricity suppliers and consumers in an automated fashion to ameliorate the efficiency, reliability, and economics of electricity. 42,000



monthly Google discovery highlights the concept's popularity. Smart Grids will also be able to detect sources of power outages more swiftly and at personal household levels like near by solar panel, making possible distributed energy system.

9.7. IoT in Industrial Internet

The industrial internet is the new buzz in the industrial sector, also termed as Industrial Internet of Things (IIoT). It is entitle industrial engineering with sensors, software and big data analytics to create brilliant machines. The many market researches like as Cisco or Gartner see the industrial internet as the IoT concept with the highest overall potential, its prominence currently doesn't reach the masses like smart home or wearable's do. The industrial internet however has a lot going for it. IIoT holds a great capacity for quality control and sustainability. Applications for tracking goods, actual time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain efficiency.

9.8. IoT in the Car

A connected car is a vehicle which is able to improve its own operation, maintenance as well as convenience of passengers using on-board sensors and internet connectivity. The development cycles in the automotive industry typically take two to four years, we haven't seen much buzz around the connected car yet. But it seems we are getting there. Most big auto makers as well as some brave startups are working on connected car solutions.

9.9. IoT in Lighting Control

Although a partial version of the technology has been already in the market, this disassemble itself in the fact that it integrates lighting control with mesh networking to develop huge scale, credible, wireless lighting solutions for homes. The sensors embedded can also detect the presence of people and turn off the lights in their absence. The lighting system is designed to save on energy consumption in both commercial and residential establishments.

9.10. IoT in Healthcare

IoT has different applications in healthcare, which are from remote monitoring equipment to advance & smart sensors to equipment integration. It has the capability to rejuvenate how physicians deliver care and also keep patients safe and healthy. The concept of a connected health care system and smart medical devices bears huge capability, not just for companies also for the well-being of people in general. IoT in healthcare will be massive in imminent years. IoT in healthcare is the intention of empowering people to live healthier life by wearing connected devices. The collected data will help with personalized analysis of an individual's health and provide tailor made action plan to combat the disease.

9.11. IoT in Retail

The capability of IoT in the retail sector is huge. IoT endows an eventuality to retailers to connect with the customers to improve the in store experience. Smartphones will be the way for retailers to stay connected with their consumers even out of the store. Interacting via smartphones and using Beacon technology can help retailers serve their consumers preferable. They can also track the consumer's path via a store and

ameliorate store layout and place premium products in high traffic areas.

9.12. IoT in Supply Chain

The supply chains have already been getting dexterous for a couple of years. The solutions for tracking, goods while they are on the road, or getting suppliers to commutation inventory information have been on the market for years. So while it is completely logic that the topic will get a new push with the IoT, it seems that so far its prominence remains limited. The IoT system can also process workflow and transform equipment settings to improve performance.

9.13. IoT in Agriculture

The smart farming is an often overlooked business case for the IoT because it does not really fit into the well-known categories like as industrial, health, mobility. However, due to the remoteness of farming operations and the huge number of lives tock that could be monitored the IoT could metamorphose the way farmers work. But this opinion has not yet reached large-scale consideration. Farmers are using meaningful intuition from the data to yield preferable return on investment. The sensing for soil nutrients and moisture, controlling water usage for plant growth and determining custom fertilizer are some easy uses of IoT.

Finally, in this section we are discussing various areas of IoT applications and uses in real life. I expect you had fun reading about all these powerful and potential applications of the Internet of things. There are many more areas where IoT is making an influence.

10. CONCLUSION

At the present time moment, every day the big world of internet is originate 2.9 quintillion bytes of data on a regular basis according to the statistics the percentage of data that has been originated from last two years is 92%. The Internet of Things (IoT) promises to have a big effect by adding a new dimension in the way people will interact with the surrounding things. The IoT can connect devices embedded in different systems to the internet. When objects and devices can represent themselves digitally, they can be controlled from ubiquitously. The connectivity, then helps us capture more data from more places; make sure that the more ways of increasing efficiency and improving safety and the IoT security. The Internet of Things is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are endued with unique identifiers and the efficiency to transfer data over a network without essential human-to-computer or human-to-human interaction. IoT platforms can help organizations decrease cost via make better process efficiency, asset utilization and productivity. To make a better tracking of devices and objects using sensors and connectivity, they can advantage from real-time insights and analytics, which would help them, make smarter decisions. In this paper, we survey state-of-the-art methods, architecture of IoT, classification, ecosystem, reference model of the Internet of Things (IoT) and applications in this new emerging area, also highlights some of the most important technologies. This paper's purpose to endue a substantial overview and big-picture to readers of this emerging area.



11. FUTURE WORK

For future work, we are planning to analyze Internet of Things (IoT) security and technological perspective and review the existing Internet of Things (IoT) environments.

12. ACKNOWLEDGEMENTS

The author would like to thank the reviewers anonymous for their constructive comments and that helped whit their revision to improve the resulting quality of this paper. I would like to express my gratitude towards my family and colleges for their co-operation and help me in completing this paper.

13. REFERENCES

- [1] Yusuf Perwej, "An Experiential Study of the Big Data," International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Vol. 4, No. 1, page 14-25, March 2017, DOI:10.12691/iteces-4-1-3.
- [2] Xia Feng et al., "Internet of things", International Journal of Communication Systems, vol. 25, no. 9, pp. 1101, 2012.
- [3] Kevin Ashton, "That 'Internet of Things' Thing", RFID Journal, 22 June 2009.
- [4] Zhu Qian et al., "Iot gateway: Bridging wireless sensor networks into internet of things", Embedded and Ubiquitous Computing (EUC) 2010 IEEE/IFIP 8th International Conference on. IEEE, 2010.
- [5] IEEE Standards Association (IEEE-SA). Internet of Things (IoT) Ecosystem Study, IEEE Standards Association, The Institute of Electrical and Electronics Engineers, Inc., 2015.
- [6] Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020," Gartner, 12 December 2013.
- [7] NIST Big Data Public Working Group. NIST Big Data Interoperability Framework: Volume 7, Standards Roadmap, NIST Big Data Public Working Group, NIST Special Publication 1500-7, September 2015.
- [8] Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, "A Perusal Of Big Data Classification And Hadoop Technology," International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Vol. 4, No. 1, page 26-38, May 2017, DOI: 10.12691/iteces-4-1-4.
- [9] Jeremy Crump, "Time for debate about the societal impact of the Internet of Things," The Policy and Internet Blog, University of Oxford, April 22, 2013. Retrieved: May 12, 2015.
- [10] Hakima, Chaochi. (ed.) The Internet of Things: Connecting Objects to the Web, 2010, p.252.
- [11] Holdowsky, J., Mahto, M., Raynor, M., Cotteleer, M., Inside the Internet of Things (IoT), Deloitte University Press, New York, 2015.
- [12] Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K., "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities". IEEE Wireless Communications, 20(6), 91-98, 2013
- [13] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," IEEE Software, vol. 33, no. 1, pp. 112–116, 2016.
- [14] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 5. IEEE, 2010, pp. V5–484.
- [15] S. K. Datta, C. Bonnet, N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services", 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 514-519, March 2014.
- [16] C. Zuo, J. Shao, J.K. Liu, G. Wei, Y. Ling, "Constance: An intel-ligent data lake system", IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 186-196, 2018.
- [17] Christos S., Kostas E. P., Andreas P., Giorgos K., Yutaka I. , " Architecture for security monitoring in IoT environments", IEEE, ISSN: 2163-5145, Edinburgh, UK, June 2017 DOI: 10.1109/ISIE.2017.8001447
- [18] L. Tan and N. Wang, "Future internet: The internet of things," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 5. IEEE, 2010, pp. V5–376.
- [19] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012, pp. 257–260.
- [20] H. Ning and Z. Wang, "Future internet of things architecture: like mankind neural system or social organization framework?" IEEE Communications Letters, vol. 15, no. 4, pp. 461–463, 2011
- [21] Yusuf Perwej , Kashiful H., Uruj J., Sharad S., "Some drastic improvements found in the analysis of routing protocol for the Bluetooth technology using scatternet" International Conference on Computing, Communications and Information Technology Applications (CCITA-2010) , Ubiquitous Computing and Communication Journal (UBICC) Seoul, South Korea, ISSN Online 1992-8424, ISSN Print 1994-4608, Volume CCITA-2010, Number 5, pages 86-95, 2010
- [22] Yusuf Perwej, "The Next Generation of Wireless Communication Using Li-Fi (Light Fidelity) Technology," Journal of Computer Networks (JCN), USA, ISSN (Print): 2372-4749 ISSN (Online): 2372-4757, which is published by Science and Education Publishing Vol. 4, No. 1, page 20-29, June 2017 DOI:10.12691/jcn-4-1-3
- [23] Rodrigo Román-Castro ; Javier López ; Stefanos Gritzalis," Evolution and Trends in IoT Security", IEEE Computer Society, Computer ,Volume: 51 , Issue: 7 , July 2018 DOI: 10.1109/MC.2018.3011051
- [24] Pedro Maló ; Márcio Mateus ; Bruno Almeida ; Tiago Teixeira," Measuring Data Transfer in Heterogeneous IoT Environments", EEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social



- Computing, Electronic ISBN: 978-0-7695-5046-6 , Beijing, China, Aug. 2013 DOI: 10.1109/GreenCom-iThings-CPSCOM.2013.102
- [25] Yusuf Perwej, Md. Husamuddin, MajzoobK.Omer, Bedine Kerim, “A Comprehend TheApache Flink In Big Data Environments” IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, USA, Volume 20, Issue 1, Ver. IV, PP 48-58, Feb. 2018, DOI : 10.9790/0661-2001044858
- [26] Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, “A Close-Up View About Spark in Big Data Jurisdiction” International Journal of Engineering Research and Application (IJERA), ISSN : 2248-9622, Vol. 8, Issue 1, (Part -11), pp.26-41 January 2018, DOI: 10.9790/9622-0801022641
- [27] Vinton G. Cerf,” A Revised View of the IoT Ecosystem”, IEEE Computer Society, IEEE Internet Computing ,Volume: 21 ,Issue: 5 , 2017, DOI: 10.1109/MIC.2017.3481356
- [28] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, Q. Z. Sheng, "IoT middleware: A survey on issues and enabling technologies", IEEE Internet Things J., vol. 4, no. 1, pp. 1-20, Feb. 2017.
- [29] Matthias Thoma ; Sonja Meyer ; Klaus Sperner ; Stefan Meissner ; Torsten Braun ,” On IoT-services: Survey,
- [30] Classification and Enterprise Integration ”, IEEE International Conference on Green Computing and Communications, INSPEC Accession Number: 13372142, Besancon, France , Nov. 2012
- [31] Bruno Dorsemaine ; Jean-Philippe Gaulier ; Jean-Philippe Wary ; Nizar Kheir ; Pascal Urien ,” Internet of Things: A Definition & Taxonomy”, 9th International Conference on Next Generation Mobile Applications, Services and Technologies, IEEE, Print ISBN: 978-1-4799-8660-6 , Cambridge, UK, Sept. 2015, DOI: 10.1109/NGMAST.2015.71
- [32] M. Swan, “Sensor mania! The internet of things, wearable computing, objective metrics, and the quantified self 2.0,” Journal of Sensor and Actuator Networks, vol. 1, no. 3, pp. 217–253, 2012
- [33] A. Whitmore, A. Agarwal, and L. Da Xu, “The internet of Things a survey of topics and trends,” Information Systems Frontiers, vol. 17, no. 2, pp. 261–274, 2015
- [34] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, “Role of middleware for internet of things: a study ,” International Journal of Computer Science & Engineering Survey, vol. 2, no. 3, pp. 94–105, 2011.
- [35] Rodolfo X. Gordillo , Carlos G. Romero , Sandy E. Abasolo , Michelle A. Carrera,” Testbed for evaluating reference models of Internet of Things (IoT) ”, IEEE Colombian Conference on Communications and Computing (COLCOM), INSPEC Accession Number: 14468979, Bogota, Colombia, June 2014
- [36] James P. G. Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, and Paul Smith.,” Redundancy, Diversity,and Connectivity to Achieve Multilevel Network Resilience, Survivability, and Disruption Tolerance (invited paper).” Telecommunication Systems, 56, 1, 17–31, 2014
- [37] Mauro A. A. da Cruz , Joel José P. C. Rodrigues , Jalal Al-Muhtadi , Valery V., Victor Hu,” A Reference Model for Internet of Things Middleware ”, IEEE Internet of Things Journal, Volume: 5 , Issue: 2 , Page(s): 871 – 883, April 2018
- [38] S. Yi, Z. Qin, Q. Li, "Security and Privacy Issues of Fog Computing: A Survey", Proc. Int'l Conf. Wireless Algorithms Systems and Applications, pp. 685-695, 2015.
- [39] Boyi Xu, Li Da Xu, Hongming Cai, Cheng Xie, Jingyuan Hu, Fenglin Bu, "Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services", IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1578-1586, May 2014.
- [40] Shen Bin, Liu Y., Wang X., "Research on Data Mining Models for the Internet of Things", IEEE, pp. 3-17, 2010.
- [41] Feng Chen, Changrui Ren , Jin Dong , Qinhua Wang , Jinfeng Li , Bing Shao ,” IEEE International Conference on Web Services”, INSPEC Accession Number: 12219345 , Washington, DC, USA, July 2011
- [42] Simon Jiang,” Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer)”, IEEE, INSPEC Accession Number: 15700870 , Colombo, Sri Lanka, Aug. 2015
- [43] Razzak, F. (2012) Spamming the Internet of Things: A Possibility and its probable Solution. Procedia Computer Science, 10, 658-665.
- [44] E. Welbourne, I. Battle, G. Cole, K. Gould, K. Rector, S. Raymer et al., "building the internet of things using rfid the rfid ecosystem experience", iee internet comput., vol. 13, pp. 48-55, 2009.
- [45] Shao, W. and Li, L. (2009) Analysis of the Development Route of IoT in China. Perking: China Science and Technology Information, 24, 330-331.
- [46] R. Want, "Enabling Ubiquitous Sensing with RFID", Computer, vol. 37, no. 4, pp. 84-86, 2004.
- [47] Leong et al., The Sun EPC network architecture a technical white paper, 2004.
- [48] A. C. W. Wong, M. Dawkins, G. Devita, N. Kasparidis, A. Katsiamis, O. King, F. Lauria, J. Schiff, A. J. Burdett, "A 1 V 5 mA multimode IEEE 802.15.6/Bluetooth low-energy WBAN transceiver for biotelemetry applications", IEEE J. Solid-State Circuits, vol. 8, no. 1, pp. 186-198, 2013
- [49] Felix von Reischach ; Stephan Karpischek ; Florian Michahelles ; Robert Adelman ,” Internet of Things (IOT)”, Tokyo, Japan, Dec. 2010, DOI: 10.1109/IOT.2010.5678457
- [50] F. Lassabe, P. Canalda, P. Chatonnay, F. Spies, "Indoor Wi-Fi positioning: techniques and systems" in Annals of Telecommunications, Paris:Springer, vol. 64, no. 9, pp. 651-664, 2009.
- [51] D. Martin-Sacristan, J. F. Monserrat, J. Cabrejas-Peñuelas, D. Calabuig, S. Garrigas, N. Cardona, "On the



- Way Towards Fourth-generation Mobile: 3GPP LTE and LTE-advanced", EURASIP Journal on Wireless Communications and Networking, pp. 4:1-4:10, Mar. 2009.
- [52] Mark Coates, Mike Rabbat, "Sensor Networks Part 2: ZigBee and IEEE 802.15.4".
- [53] S. Ortiz, "Is Near-Field Communication Close to Success?", Computer, vol. 39, no. 3, pp. 18-20, March 2006.
- [54] Manijeh, Amene, "A Wireless Sensor Network solution for precision agriculture based on Zigbee Technology", Scientific Research Wireless Sensor Network, vol. 4, pp. 25-30, 2012.
- [55] Arampatzis, T., et al. (2005) A Survey of Security Issues in Wireless Sensors Networks, in Intelligent Control. Pro-ceeding of the IEEE International Symposium on, Mediterrean Conference on Control and Automation, 719-724.
- [56] Richard Boire, "Artificial intelligence(AI), automation, and its impact on data science", IEEE International Conference on Big Data (Big Data), Boston, MA, USA, Dec. 2017
- [57] Yusuf Perwej , Firoj Parwej, "A Neuroplasticity (Brain Plasticity) Approach to Use in Artificial Neural Network", International Journal of Scientific & Engineering Research (IJSER), France , Vol.3, Issue 6, June 2012, Pages 1- 9, ISSN 2229 – 5518.
DOI: 10.13140/2.1.1693.2808
- [58] Daniel Camps-Mur, Andres Garcia-Saavedra, Pablo Serrano, "Device-To-Device Communications with Wi-Fi Direct: Overview and Experimentation", IEEE Wireless Communications, vol. 20, no. 2, June 2013.
- [59] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, "Internet of Things for Smart Cities", IEEE Internet Things J., vol. 1, no. 1, pp. 22-32, 2014
- [60] S. Li, L. Da Xu, S. Zhao, "The internet of things: a survey", Inf. Syst. Front., vol. 17, no. 2, pp. 243-259, 2015.
- [61] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A vision architectural elements and future directions", Future Generation Computer Systems, 2013.