Journal of Engineering Science and Technology
Vol. 14, No. 3 (2019) 1717 - 1750

INTERNET-OF-THINGS: GENESIS, CHALLENGES AND APPLICATIONS

PRIYA MATTA*, BHASKER PANT

Computer Science and Engineering, Graphic Era Deemed to be University
566/6, Bell Road, Clement Town, Dehradun, India
*Corresponding Author: mattapriya21@gmail.com

Abstract

As of now, we are in an age where every object is a smart object. A smart object is an object that has embedded electronics and connected to the internet. In other words, specifically, we are in the era of Internet-of-Things (IoT). The concept of Internet-of-Things is to interconnect various things making use of electronic devices such as sensors and actuators. Its basic aim is to fit each and every physical and logical object into the computing world. It emphasises the assimilation of the internet into every single entity, that can exist in living or non-living, tangible or intangible, physical or logical form. This paper addresses the current trends, major research challenges and application domains in the field of Internet-of-Things (IoT). This work covers the various viewpoints of several academicians, practitioners, researchers and organisations about IoT. This paper aims to classify, compare, and encapsulate the challenges, demanded solutions and suggestions related to IoT. Research challenges are classified as Technological, Environmental, and Societal. The technological challenges are further classified into architecture and heterogeneity, resource management, efficient data handling and security. The target of this research paper is to deliver a better awareness of IoT by bringing out the major subjects and relevant issues associated with its implementation.

Keywords: Application domains, Challenges, Internet-of-things, Sensors.

1. Introduction

In last two decades, technology has made a tremendous improvement, especially in interconnections of computers, devices, personals and objects. At the same time, computer networks have matured with significant enhancements. The best example of this advancement is the advent of the most remarkable network that is the Internet. With the arrival of the Internet, a number of innovative and appealing technologies are also emerging and incorporating themselves into the computing world. Naming few of them are distributed computing, grid computing, cloud computing and ubiquitous computing.

The improvisation and extemporisation of technology and computing methodology are driving the world towards another astonishing paradigm that is Internet-of-Things (IoT). In 1999, Kevin Ashton, a British entrepreneur coined the term IoT when he was working with Auto-ID Labs.

International Telecommunication Union-Global standard initiative ITU-GSI [1] proposed that IoT is a principal integral out of five projecting and noticeable research domains, which are, mobile-computing, wireless-sensor-networks, pervasive-computing, IoT and, cyber-physical systems. IoT is an emerging field, which is wrapping up and encompassing the entire world under its own umbrella.

This work explains the status of IoT in current as well as the future scenario. After going through the introduction of IoT, we deliberated a number of definitions in section 1. Genesis and Growth of IoT has reflected in Section 2. Section 3 is all about the various challenges, a detailed survey of some of the discovered challenges as well as proposed solutions in the field of IoT. This section gives a prominent elaborative study of Technological, Societal and Environmental Challenges. Subcategories of research challenges are also highlighted in the same section. This paper covers a comprehensive analysis of application domains of IoT in Section 4. Subcategories of application domains are also elaborated in the same section. The paper ends up with the conclusion in Section 5.

Definitions of IoT

Different researchers, academicians, organisations define IoT in their own way, with their own perspectives.

Definition 1: ITU-GSI [1] has defined IoT as "the network of physical objects - devices, vehicles, buildings and other items - embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data". The notion of IoT is to interconnect various things making use of electronic sensors. Its major goal is to get embedded and involved in every aspect of the real world. Attainment of this goal finally brings us where we ever want to reach, i.e., increased efficiency, availability and optimised use of resources.

Definition 2: According to China Communication Standards Association (CCSA) [2], IoT is "a network, which can collect information from the physical world or control the physical world objects through various deployed devices with the capability of perception, computation, execution and communication, as well as support communications between human and things or between the things by transmitting, classifying and processing information".

Definition 3: According to International Telecommunication Union (ITU) [3] standards, IoT is "a global infrastructure for the information society that enables advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies". In terms of connectivity, ITU-T realised IoT as a network with anyplace and anytime connectivity for anyone or anything.

Definition 4: According to Vermesan et al. [4], the realisation of IoT can be extended to 6A's connectivity: connecting people and objects, anytime, from any place with anyone or anything, while, preferably by means of any network or any service.

Definition 5: Lee et al. [5] have communicated that the well-known body related to the world of internet namely Internet Engineering Task Force (IETF) has defined IoT as "a worldwide network of interconnected objects uniquely addressable based on standard communication protocols".

Definition 6: According to Yan et al. [6], understanding, IoT is "a paradigm, whereby the existing networked devices connect to the real-world objects such as home appliances, vehicles, and health-care". Here objects are smart objects, which are capable of sensing the other objects lying around them and capable of communicating with them by means of the Internet.

Definition 7: According to Chen et al. [7], the IoT is "an intelligent network, which connects all things to the Internet for the purpose of exchanging information and communicating with the information sensing devices in accordance with agreed protocols". They also realized IoT as an expansion of existing interaction among applications and people from a very naïve viewpoint of "Things" for communication. These "Things" can be treated as a combination of hardware, software, data, and service.

Definition 8: Hendricks [8] refers to IoT as "a world-wide network of interconnected objects uniquely addressable based on standard communication protocols whose point of convergence is the Internet".

Definition 9: In 2005, according to International Telecommunication Union (ITU) [9] Report, "IoT will connect the world's objects in both a sensory and intelligent manner through combining technological developments in item identification (tagging things), sensors and wireless sensor networks (feeling things), embedded systems (thinking things) and nanotechnology (shrinking things)".

Definition 10: The Europen Research Cluster (IERC) [10] describes the IoT as: "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."

After going through findings and views of various academicians, researchers, and organisation, it can be concluded that IoT is a wide range collection of processes, interconnected devices and their supporting technologies, along with the environment they all exist in. The IoT permits different objects to get detected, identified and controlled distantly across the existing networks. It results in the generation of prospects to integrate the physical entities into the information world and therefore ensuring better efficiency, significant accuracy, and financial

yield. IoT can also be treated as an illustration of cyber-physical-systems, as it incorporates the paradigms of a smart city, smart home, smart transportation and even smart traffic.

In the light of the above definitions, IoT is defined as "a paradigm with a notion of enabling the things (physical entities, e.g,: human, car, animal, mirror, bulb, plant, etc.) to communicate with each other, to transfer and receive the information (read-only data), through the use of underlying network (wired or wireless), supporting technologies (e.g., ZigBee, Bluetooth, Wi-Fi, etc.), required sensors, actuators and computing devices, and finally respond back in a way that requires least or negligible human intervention".

The above-mentioned things may be any living or non-living thing, they may be some devices, vehicles, or machines; they may be a human being, an animal or a tree also. These things are definitely smart things, having electronics and computing capabilities embedded into them. Here communication means transmitting the data from things, sensing data using sensors, and transferring the data into actuators. In the context of IoT, the data being transferred is read-only data. This read-only data is also termed as telemetry. This interconnection and integration of things, data, networks, sensors, actuators, and computing devices results in an IoT infrastructure.

2. Genesis and Growth of IoT

In today's era, the world can be retreated as either physical or the information world. These two terms physical and information world are not disjointed, as they are glued together via the interface "end user" and fused together via the linkage of "Internet". This conjunction is leading towards the genesis of the paradigm of IoT. The evolution and growth of IoT rely on the invention of new technologies and strengthening of existing ones. These technologies range from wired networks, wireless networking, sensor networks, Radio-Frequency Identification (RFID), nanotechnology, embedded software, communication protocols and ubiquitous computing. The highlight of this evolution of IoT is, instead of creating a novel global network; this paradigm uses the Internet as an underlying platform. Over the layered Internet where one computing device can communicate with the other computing device, there evolve IoT. IoT links each object, turning them into a smart thing. This transformation of a thing into the smart thing, object into a smart object, and appliance into a smart appliance is achievable by embedding sensing, transmitting and computing capabilities into them.

The two most impressive, meaningful and contradictory statements given by Kevin Ashton in 2006 and 2009 respectively [11] as:

- "After the World Wide Web (the 1990's) and the mobile Internet (the 2000's), we are now heading to the third and potentially most disruptive phase of the Internet revolution - the IoT".
- "The IoT has the potential to change the world, just as the Internet did. May be even more so".

According to Kevin Ashton, IoT is a disruptive phase of Internet technology, as IoT can make the end user able to access sensitive information, which he/she could use inappropriately or cleverly. On the other hand, Kevin Ashton himself

praised the competence and potential of the technology if implemented successfully and completely.

According to the Cisco Internet Business Solutions Group (IBSG) [12], "IoT is simply the point in time when more things or objects were connected to the Internet than people." In 2003, the population of the world was calculated to be 6.3 billion, while connected devices were only .5 billion. Similarly, in 2010, the figure was 6.8 billion for population and 12.5 for the connected devices. In 2015, the population became 7.2 billion while connected devices count reached 25 billion. In 2020, the population will touch the figure of 7.6 billion, and connected devices will reach 50 billion [12].

Based on the above facts and figure, the ratio between population count and the count of connected devices can be calculated. This calculation and generated ratios are given in Table 1 and are shown in Fig. 1.

Table 1. Ratio of population with connected devices.

Year	Population (in billion)	Connected devices (in billion)	Ratio
2003	6.3	.5	.08
2010	6.8	12.5	1.84
2015	7.2	25	3.47
2020	7.6	50	6.58

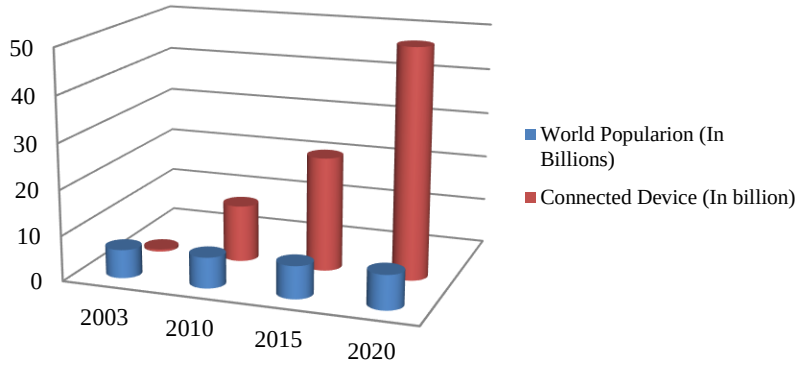

Fig. 1. Comparison between world population and connected devices.

In this section, the evolution of IoT has been discussed. The evolution of IoT can be deliberated as gradual changes in technology along with time. Initially, the computing world had only standalone machines. Then came the era of networking, to fulfil the requirements of sharing, sharing the resources and information. The interconnection of computing devices finally results in emergence of most appealing and successful network, the Internet. The Internet is composed of many intranets, individual computing devices, and organisations. The next advancement

in technology was wireless connectivity. The advent of wireless connectivity and miniaturisation of computing devices lead us towards mobile computing. Availability of all these technologies along with electronic equipment like sensors and actuators brought us in a phase of technology, where every object is assumed to be sensed and has some computing capabilities and finally resulting in the era of IoT. This progression can be shown pictorially in the way presented in Fig. 2.

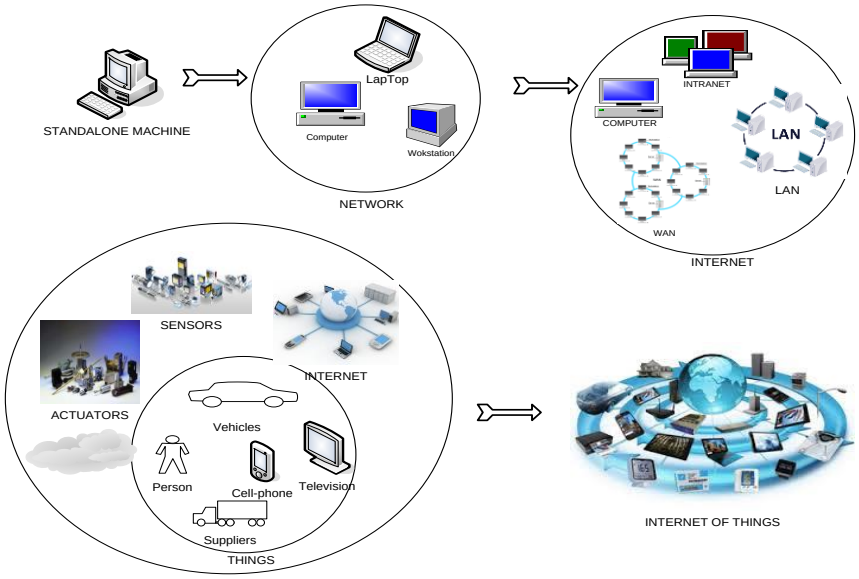

Fig. 2. Genesis of IoT.

One of the most significant drivers to run the paradigm of IoT is its pervasive presence around the people, its ability to quantify, recognise, realise and most importantly change itself according to the environment or modify the environment consequently. In the near future, the world would seem to be interconnected linkage or web of all the existing entities. Nowadays the efforts are to indulge computing power as well as the ability to connect to each and everything. IoT is not only powered by the innovations in technology and communications, but it also includes different things incorporated into day-to-day life. These things may be tangible or intangible, visible or invisible, computing device or a non-computing one. Things may belong to a private organisation or a public one. These things may vary from simple things like furniture, food material, and clothes to complex devices like cellular phones, television, and other electronic appliances [13, 14]. All these mentioned objects and entities are able to properly communicate with each other, playing the role of Sensors, finally reaching the joint objective and accomplishing the common task. The most critical aspect of IoT is its impact on the day-to-day life of apparent users [9, 15-17].

IoT will definitely improve the quality of life by proposing new services to convert cities into smarter cities and improving the interaction between people and IoT devices/services. IoT has an extraordinary impact in both the domains of a home as well as working place. It has a very bright future while supporting e-health, aided-living, smart transportation, smart traffic and even smart city. The

business scenario cannot be left untouched from its impact and consequences. After observing all these considerations, the US National Intelligence Council has declared IoT as one of the six potential technologies attracting US interests on the way to 2025 [14].

After observing the facts and figures, this is also concluded that the count of interconnected devices surpassed the count of people in 2010 and it is expected that a number of interconnected devices will reach the value of 25 billion by 2020. Such a huge count suggests that IoT will be one of the main sources of big data [18]. Such an exponential increase in the vastness of the field and complications in its implementation make it an exciting field for research too. It is also observed that today applications of IoT are also turning towards social life applications such as smart-grid, smart-transportation, smart-security, and smart-home [19].

The quantification of IoT is done by studying and analysing the reports given by various experts and organisations. Experts predicted that there will be approximately 50 billion objects existing on the IoT by 2020 [14]. According to Gartner [20], (a technology research and advisory corporation), the count of devices existing in the IoT will be 30 billion by 2020. On the other hand, ABI Research predicted that the total number of devices connected to IoT wirelessly will be more than 30 billion [21]. In another survey done by Pew Research Internet Project, it is concluded that the IoT, embedded computing, corresponding dynamic system and wearable computing will have extensive and the favourable effects by 2025 [22]. As a result, it is quite visible that, the IoT will consist of an enormous count of devices being linked to the Internet.

In 2015 budget, UK Government allocated an amount of £40,000,000 to do the research in the domain of IoT. The British Chancellor announced that the IoT is the next phase of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances [23]. Arseni et al. [24] proposed that the IT paradigm referred to as the Internet-of-Things (IoT) targets to assemble each and every technological entity that is able to communicate, in the same box. According to Miorandi et al. [25], the IoT can be thought of as a technological paradigm integrating traditional networks and networked entities. In fact, the evolution of IoT will attain a form of service provider. The academicians, researchers and various organisations (private sector as well as government bodies) are looking forward to constructing a suitable, user-friendly, convenient and efficient environment to live-in and to work in. This revolution of advancing technology, accessible networking and availability of embedded computing devices figures out IoT as a fruitful area of research in the coming future.

3. Research Challenges and Related Study

From the perspective of an end user and from the perspective of IoT stakeholders, the challenges, as well as their solutions, may vary. It is realistic to assume that the current state of IoT may lead to a numerous range of challenges. In this section, our purpose is to examine and review some of the foremost challenges that must be focused to implement IoT effectively and productively.

Matta et al. [26] categorised the challenges in the domain of the IoT paradigm into three broader areas. These are namely Technological Challenges, Societal

Challenges, and Environmental Challenges. These challenges are elaborated with their subclassification in *Appendix A*.

3.1. Technological challenges

Technological Challenges are further classified into four broader categories: Architecture and Heterogeneity, Resource Management, Efficient Data Handling, and Security and Privacy.

3.1.1 Architecture and heterogeneity

Many researchers have attempted to define various architectural models to implement IoT; some of them are typically applied to a particular application area. Castellani et al. [27] have given an architecture design, particularly for a smart office application. This model aims at the interconnection of wireless sensor networks and actuator networks to the Internet as a web service. These services include such as door entree control, to grant permission to an authenticated person and as a result, it requires a reliable network and some identification technologies (e.g., RFID). Their model is comprised of three kinds of nodes, namely Base Station Node (BSN), Mobile Node (MN), and Specialized Node (SN). Each kind has its own attributes based on its mobility, its operation range, and its specialisation. A BSN is a static node; say an IPv6 sink or IPv6 router. It provides direct connectivity to the Internet. An MN is an external node, say wireless dongle. It focuses on compatibility issues towards network protocols and network configurations. Third and the core portion of the complete architecture is an SN. It is a specialised node to deliver the specific service(s), say temperature readings, water level readings.

Beier et al. [28] offered the EPC (Electronic Product Code) global IoT architecture. Its main focus is towards RFID networks and smart logistics systems. This proposal is based on the concept of Discovery services. Discovery services offer a service that correlates the information of RFID-enabled products during the process of data exchange in a supply chain management practice. Discovery service consists of a well-defined database and a collection of web service interfaces.

One additional service is proposed by EPCglobal, namely Object-Name Service. It is treated as an instance of a discovery service. They also suggested to generate an EPC number, from the appropriate domain name and then retrieve a record of all EPCIS (electronic product code information services) using the already existing DNS. Whenever an organisation has to use Discovery Service, it has to get authorised by an authoritative group. After getting authorised, it will get a signed certificate from another trusted group. Afterwards, all the transactions made by the organisations will be done via this certificate. The 5 major contents of this certificate are:

- EPC number of the product,
- Certificate of the company who's EPCIS submitted the record,
- URL of the EPCIS to indicate that it had custody of the item,
- Timestamp when this record was inserted,
- Visibility, a flag indicating if the record can be shared with anybody or not.

To implement the paradigm of IoT, many researchers have proposed a number of layered architectures. Gronbaek [29] and Dai and Wang [30] have given OSI-model like architecture. Tan and Wang [31] suggested that the architecture will support ubiquitous services on an end-to-end basis. Dai and Wang [30] proposed an architecture that consists of four layers, namely Things layer, Adaptation layer, Internet layer and Application layer.

Tan and Wang [31] proposed a five-layered architecture for the IoT. They proposed that there are five layers, which can represent an IoT system completely. These are the Application layer, Middleware layer, Coordination Backbone layer and finally, the fifth layer again consisting of Existing Alone Application System, Access layer, Edge Technology layer.

Ma [32] suggested that, before designing the architecture of IoT, one has to consider the different viewpoints of its users, developers, various service providers and the network providers. Taking these into consideration, various interfaces, supporting protocols and required standards are defined. According to Ma [32], the IoT-architecture can be divided into four different layers: i) Object Sensing layer; ii) Data Exchange layer; iii) Information Integration layer and iv) Application Service layer. The first layer, i.e., object sensing layer is responsible for sensing the things and collecting the required data; the second layer, i.e., the data exchange layer is responsible for the transparent transmission of collected data; the third layer, i.e., the information integration layer is responsible for different tasks related to the data acquired. These tasks are cleaning, and fusion of random and ambiguous data collected from the network and finally shape that fused data into meaningful information. The last layer, i.e., the application service layer is responsible for providing the content services to the end users.

Bandyopadhyay and Sen [33] proposed an all-purpose five-layered architecture to represent an IoT system. The five layers are: i) Edge Technology layer; ii) Access Gateway layer; iii) Internet layer; iv) Middleware layer; and v) Application layer.

Sarkar et al. [34] offered that three-layered architecture to completely represent the IoT infrastructure. These layers are i) Virtual Object Layer (VOL); ii) Composite Virtual Object Layer (CVOL), and iii) service layer (SL). VOL handles object-virtualisation, CVOL handles, service composition, and execution, and SL handles service creation and management.

Some other researchers have provided different directions towards the design and growth of IoT architectures. Ning and Wang [35] have designed and developed the IoT architectures based on Human neural system and SOFs (social organisation framework). They have proposed two models for IoT architecture namely i) Unit IoT, and ii) Ubiquitous IoT. Unit IoT gets its motivation from a man-like nervous (MLN) model. This emphasises to provide solutions for different applications using the MLN model. Here the three major components are M&DC (Management and Centralized Data Centre) resembling the brain, DCN (Distributed Control Nodes) resembling the spinal cord, NoS (Networks and Sensors) resembling nerves. The Ubiquitous IoT gets its motivation from a social organisation framework (SOF). It can further be categorised as Industrial IoT, or National IoT, or Local IoT, depending on its range and connectivity limits.

Kovatsch et al. [36] have offered centralised architecture to segregate the device heterogeneity from application development. They proposed the concept of a thin

server. Here thin server is a device enacting as a server, but none of the application logic resides on this server. It supports the promotion of an application layer that seems to be a web-like layer.

Most of the proposed architecture is meant for specialised application and thus does not support all type of environmental and industrial applications. These architectures do not discuss any issue regarding how the different layers will work and interact with each other to exchange the data and information. If every object is connected and things can exchange information by themselves, then the traffic and storage in the network will increase very rapidly. None of these offered any improvement to control high traffic of data.

Heterogeneity is one of the key attributes of an IoT system. IoT system is composed of various types of device, various network topologies, network configuration, and various forms of data representation. It is a challenging task to support this heterogeneity in an efficient manner so that all the devices can be managed properly. According to Baraniuk [37], traditional solutions may suffer a variety of functional degradation and can turn out to be quite complex solutions, while implementing the heterogeneity.

Another challenge discussed by them is that, as the IoT systems applications involve the usage of the Internet completely, and therefore they are more prone to the vast range of adversaries. According to Hendricks [8], a generalised heterogeneous architecture is required to support the heterogeneous environment consisting of various types of devices, underlying networks, their configuration, their topologies, etc. The single reference architecture cannot be the best solution for the heterogeneous environment of IoT.

Scalability in architecture is another issue handled by some authors. Waldner [38] clearly mentioned that as IPv6 protocol provides an exceptionally big address space, therefore future internet applications will adapt it to handle the extremely large range of objects. They clearly specify that the 128-bit IPv6 addressing scheme is currently being deployed in many applications as it is able to accommodate near trillion addresses. Therefore, the scalability in IoT can be achieved via the usage of the IPv6 addressing scheme.

Chen et al. [7] also encouraged the idea of having multiple architectures; those should follow the property of openness. According to them openness and versatility are two important attributes of architecture. When we talk about the architecture of an IoT system, we cannot restrict our self to a single technology, single topology, a single type of computing device, a single type of platform, same transmission speed. Therefore, it is concluded here that the major concern over here is to design, not a single architecture but a set of architectures.

3.1.2. Resource management

As it is known that IoT is a system that is constituted by a number of interacting nodes, these nodes are processes as well as resources. To exploit the maximum capacity and benefits of IoT, all the resources related to IoT must be managed in an efficient and well-planned manner. Numerous resources comprising of human beings, soft agents, smart objects, sensors, as well as actuators, will be connected and communicate with each other to utilize the paradigm of IoT to its fullest.

According to Zhang and Sun [39], "in the near future, humans will be surrounded by trillions of machines that interconnect with each other and can interact with or understand the physical space". According to Sundmaeker et al. [19], "how to manage, integrate, and exploit these multiple, heterogeneous, or even distributed resources is one of the primary challenges for IoT".

Many proposals have been generated by researchers for the integration and management of heterogeneous resources in a distributed and networked environment. Zhang and Sun [39] offered a model to manage and organize the different resources for an IoT system. This model is named as Semantic Hyper Network Model. Here resources and their relations are presented in the form of a hypergraph. All the resources are represented by vertices and similarly, edges are used to represent their relationships. All the nodes and links are semantic nodes and semantic links. In the case of a semantic node, it is represented as a pair of attribute and its value, i.e., (*a, v*), for every attribute of a node. In case of a link, it is represented as a triplet of the source node, a destination node, and semantic relation, i.e., (*s, t,* rel).

The representation of a semantic hyper-network is offered as SHN = (N, L), where *N* is the set of semantic nodes (hyper-nodes) and *L* is the set of semantic links connecting these semantic nodes in N. Another two notations used are level and size defined as the max time of recursion of semantic hypernodes in SHN and the number of semantic nodes in the SHN, respectively. They have also discussed six operations on hypergraphs, namely split: only hyper-node and its contents are displayed, Background: all the nodes other than the selected one are shrunk, Simplification: nodes inside the selected hyper-node are hidden, Expansion: nodes inside the selected node are expanded, Extraction: some subset of the complete SHN is extracted, Filtering: some of the semantic links are partially selected, and Hierarchy: All the nodes are placed in a form of a tree. They also compared their proposed SHN model with an existing Semantic Link Network (SLN) model, which is a semantic data model using relational reasoning. They claimed that the SHN model can represent the relations between entities in a natural way, and therefore actually support the necessity of an IoT system.

Lopez et al. [40] proposed three different concepts for the management of resources in IoT. These are namely i) clustering; ii) software agents; and synchronization techniques. Helsinger et al. [41] also approved that the task automation for devices as well as end users can be achieved via software agents. They proposed Cougaar as a scalable and distributed multi-agent architecture to support resource management in an IoT system. The main constituents of Cougaar are Cougaar Component Model (CCM), plugins, Message Transport Service (MTS), Blackboard, persistence, naming service, community, service discovery, servlets and logical domain model.

The CCM is a module that is responsible for loading and managing the software elements referred to as Components. A plug-in is described as a software module that forms the application logic, to be added into an agent. The MTS is a service that manages the inter-agent communication. The communication among the different components of a Cougaar agent is accomplished by a module called Blackboard. To recover from various kinds of failures, Cougaar has a provision of Persistence mechanism. White Pages (WP) service forms the Naming service in Cougaar. Its basic task is to map the agent name to the corresponding network

address. A set of agents that share common functionality and organisational requirements is called Cougaar Community. To support the proper consultation among various consumers and application providers, a Cougaar has a dedicated component, Service Discovery (SD). Other basic components are Servlets. The Cougaar Logical Domain Model (LDM) is responsible for the development of required application data ontologies (Domains).

Again, in the year 2011, Lopez et al. [42] proposed Smart Object framework. This framework incorporates RFID, Sensor Technologies, Object ad-hoc Network, Embedded Object Logic, and Internet-based information Infrastructure to support the concept of IoT. This framework is capable of identifying and monitoring the status of things, and therefore the structure of the network is decided accordingly. Objects are cooperating and therefore can manage their resources effectively. In this framework, the presence of well-defined interfaces can make the users able to avail object data easily.

Yu et al. [43] proposed a specific architecture for a specific IoT application. They proposed the use of cloud architecture for the smart vehicular networks. On the basis of different opportunities and various challenges of cloud computing, they designed a hierarchical architecture to implement smart vehicular networks. They rely on the concept of sharing resources. These resources include computing devices, storage devices, and even the bandwidth. Resource management is the main focus of their proposal. The proposed architecture is comprising of three layers namely, i) the vehicular cloud; ii) roadside cloud; and central cloud. Different cloud services and resources are used by the mobile nodes of the network, which are vehicles. The approach used for allocation and deallocation of the resource is Game-Theoretical Approach.

Lopez et al. [40] have proposed that resources in IoT can be managed by using techniques like clustering, software agents and even with the help of synchronisation techniques. According to them, data synchronizations techniques are also helpful in maintaining multiple copies of data related to objects in an IoT system. Helsinger et al. [41] too agreed that job automation in a large and distributed environment can be achieved by software agents.

After going through these papers, it is concluded that the storage is not implemented in many of these proposals, and consequently, there is no support for data management, therefore it can become an issue to be worked on. Another point is the network size supporting an IoT may be small (in the case of a smart home, smart retail) or medium (smart city, smart traffic, smart agriculture) or large (smart forest, smart water, smart transportation). Therefore, in case of a large network size, we have to definitely work on the shortest route between two nodes. As some of these resource management approaches are for a specific application, they can't handle other application domains of IoT. So, an improvement can be made, and a generic model with resource management can be worked out.

To improve the interoperability among various devices, heterogeneous resources in a distributed environment, the IoT requires a wide variety of open architectures, supporting efficient resource management. Therefore, allocation and reallocation of resources, as well as scheduling of a resource among a number of requesting processes, becomes a critical issue of research in an IoT system. Another aspect under consideration is concurrent access to the resources. Here in an IoT

system, there may be the situations where two or more entities (it may be any, a user, a process, a service providing interface, or a sensor itself) may try to acquire the same resource at a moment of time. In IoT, the resources (it may be a file, a device, a web page, a data value, software, hardware or a sensor again) are shareable resources. Shareable resources are those resources which can be used by two or more processes. These can be further categorised as:

- Shareable exhibiting cooperation, and
- Shareable inhibiting cooperation.

The first category is one where the resource can be accessed and utilized by two or more processes at the same time, while the second category does not allow concurrent access. When one thinks of a sharable resource, if the resource is not handled and accessed properly, it may get corrupted, or can reach to some inconsistent state. Therefore, to avoid such inconsistency, one must provide the mutual exclusion among the nodes while accessing the resource.

Using a resource in a mutually exclusive manner refers to the way that when one node (thing/ process/ user) is using the resource, no other node can access that resource. When the resource is released, it can again be used by some other node.

3.1.3. Efficient data handling

As far as any paradigm is concerned, one of its major components is data. This data may be transformed data, generated data, stored data, and data in the transit. In the case of IoT, data collection forms a major challenge. Many researchers are now and then discussing the importance of data mining in the field of IoT. According to Ma [32], one of the biggest problems in the field and realization of IoT is "Data exchange among large-scale heterogeneous network elements". More intensive information perception is required to fight with the uncertainties like non-uniformity, inconsistency, inaccuracy, and discontinuities. Ma [32] also offered the view that it is very critical to handle the exchange of data within a vast heterogeneous network. Another issue they discussed is of integrating the random data and information towards a meaningful one. According to Stankovic [44], the major problem is to handle the noisy and real-world data, to interpret that acquired data, create knowledge out of that. Another issue is the development of suitable inference techniques that are free from the shortcomings of earlier proposed schemes.

Kawamoto et al. [45] highlighted the notion of data collection. They actually discussed the authentication model, but their major focus is on data gathering. According to them, a collection of data from various heterogeneous simultaneously is a difficult task to accomplish. They also proposed a model for data collection, i.e., Computer Assisted Mass Appraisal (CAMA) Based Data Collection Model. According to them, as the range of every access point is quite big, this becomes very much difficult to acquire data from them simultaneously. Therefore, they proposed cyclic fashion to collect the data from a limited number of devices. According to Zhang and Sun [39] observation, the major problem of data handling is data storage, as it directly or indirectly depends on the storage capacity of particular sensors. Therefore, here in IoT, one cannot implement traditional approaches to data handling.

Tsai et al. [46] emphasised on data mining in relation to the Knowledge Discovery in Databases (KDD) for IoT. They suggested three primary areas of attention are i) objective; ii) characteristics of data and iii) mining algorithm. They have defined them as *O, D,* and *A.*

- Objective (*O*): The first step is to identify and specify the problem. It may include suggested assumptions, encountered limitations, and defined measurements regarding the problem.
- Data (*D*): Next and an unavoidable component in case of IoT are data. It attributes like its size, its mode of presentation and its distribution.
- Mining algorithm (*A*): Finally, one has to determine, which data mining algorithm has to be implemented, after going through the above two requirements.

According to Farooq et al. [47], in IoT, the data being collected are from various devices, using various prevailing technologies. This data used to flow among the devices. Therefore, much more care is required towards handling and mining this multidimensional data.

In this work, the data related to IoT is classified into three categories.

- "Data stating things": This category comprises of the data that defines the objects and describes their attributes. The attribute may be their unique identification, physical location, state (idle or busy, available or not), ownership if required, mode of access, etc.
- "Data produced by things": This data comprises of the data produced or transferred by objects.
- "Data absorbed by things": This data comprises of the data sensed and captured by sensors.

Efficient and secure management of this data formulates a major issue of research in the field of IoT.

3.1.4. Security and privacy

As IoT is built based on the Internet, security concerns of the Internet will also show up in IoT. These can be broadly classified as i) Authentication policies (for both the devices and the services); ii) Security of data (both static and dynamic) and iii) Privacy policies.

Machara et al. [48] recognised one of the fundamental subjects: Privacy. They identified four different dimensions of privacy:

- **Purpose**: It refers to the objective of the data being used.
- **Visibility**: It refers to the authorised people to access data.
- **Retention**: It refers to the time period for which, data is kept alive.
- **Granularity**: It refers to the level of detail at which, the data is delivered.

Security during sensing the data raises another point of discussion and decision.

Matta et al. [49] in their paper focused on the security of data in an IoT system. They proposed a generalised and multidimensional security model to handle the stored data more securely.

Commonly, users deal with the sensing information in order to make decisions in different application fields. According to Fazio et al. [50], accessing these pieces of data in a secure way is fundamental. Hardy and Tim O'Reilly [51] mentioned that IoT is trying to put all the types of objects and devices together on the Internet and making them able to serve various types of applications, therefore various tools supporting dynamic security are required. Henceforth, security tools and measures for mobile devices form a vital issue in the IoT paradigm. Data acquisition in IoT applications also generates significant security concerns. Three different threats can be identified in relation to data acquisition. These are: Data being transferred from one IoT device to other, data being transferred from IoT device to third party and vice versa.

Tsai et al. [15] suggested that privacy and security are two upcoming research issues in the paradigm of IoT. According to Agarwala et al., one can achieve a level best security in a system, but users can feel uncomfortable when it is about their privacy [52]. For example, if a healthcare application is discussed, patients can feel uncomfortable when their behaviour, types of disease, their reactions are disclosed. According to Cardwell [53], "there are some people in the commercial space who say, 'Oh, big data - well, let's collect everything, keep it around forever, we will pay for somebody to think about security later'. Many researchers have recognized that all the participants of IoT came across a variety of privacy challenges. These participants may be investors, application developers, sponsors, and even consumers. Perera et al. [54] explained that the various difficulties identified in the report are from the following:

- User consent: User must have given his consent to access the data.
- Freedom of Choice: This freedom is for both privacy protocols and supporting standards.
- Anonymity: Behaviour of things and transmission of data should be based on the user's profile.

A research team of the National Science Foundation and the University of Arkansas at Little Rock discovered that the privacy of households using smart home devices could be compromised by analysing network traffic [55]. According to Steinberg [56], a number of smart things, i.e., the internet enabled devices including televisions, cameras, and kitchen appliances can already "spy on people in their own homes".

Some important research questions [57] that should be addressed include:

When controlling an appliance at home, how are the user's actions protected to ensure no malicious application overtake the controls without the user's intention?

When checking home controls, what policies and mechanisms can ensure the information presented to a user is trustworthy and not presented by a malicious process?

Cost is the next issue. Security in collaboration with the cost forms another issue or challenge to be worked on. According to Chen et al. [7], there is a requirement to implement the security measures for handling security and privacy, but at a low-cost. Whenever security is talked about, it can be correlated to the unique identification of the user or the device. In order to be a part of the IoT system, every device, or human being or an object (physical or virtual) must possess some unique identification.

Aggarwal and Das [52] and Kosmatos et al. [13] also focused on the security issues related to RFID system with reference to IoT. Particularly due to the rapid growth of IoT, the cyber attacks are not virtual threats nowadays, rather they are emerging as a real-world threat. According to Vylegzhanina et al. [57], Security solutions for mobile devices and Dynamic security tools to prevent cross-process privilege escalation attacks involving user manipulations and intermediate network services, as they interact with their environment make the critical issues in case of an IoT system.

Kim [58] suggested architecture to fulfil the purpose of IoT security. He identified a Secure and Efficient Code Dissemination Protocol for the IoT and one Reliable and Secure Multicast Protocol. In this architecture, the perception layer comprises various securities including RFID security and WSNs security. Transportation layer comprises other securities including access network security, core network security, and local network security. The application layer comprises two fragments including application support layer and the particular application. The security in the support layer includes middleware technology security, cloud computing platform security and so on.

As mentioned by Jing et al. [59], that there are three different layers in IoT, similarly, they mentioned that one has to ensure security in all the three layers. Segmental and sectional security for each layer is of extreme importance as well as entire and intact security have to be taken care equally. Some researchers focused on one aspect of security, i.e., authentication. Kawamoto et.al [45] have discussed authentication in terms of location-based authentication. According to them, as the data collected and processed is in large quantity, and this data is being collected from various devices under varied ownership, therefore authentication must be taken proper care in IoT.

Barreto et al. [60] gave an authentication model for IoT. The authentication model is given in Fig. 3.

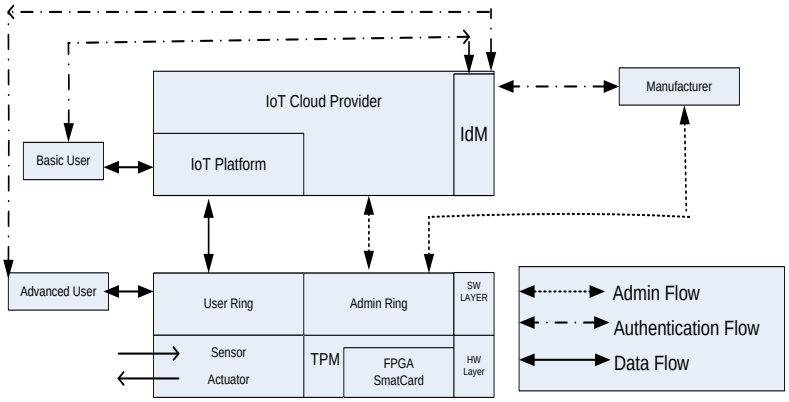

Fig. 3. Authentication model for IoT cloud [60].

This model basically categorises the user's request into two categories, namely: i) Direct access to the IoT services, and ii) Access to the IoT services via Cloud provider. Users are also categorised as basic users and advanced users. Exchange

of authentication assertions is being done between producer and consumer. As a response to increasing concerns over security, the Internet of Things Security Foundation (IoTSF) was launched on 23 September 2015. IoTSF has a mission to secure the IoT by promoting knowledge and best practice. Its founding board is made from technology providers and telecommunications companies including BT, Vodafone, Imagination Technologies and Pen Test Partners [61].

3.2. Societal challenges

After discussing the technological challenges and their inclusive literature survey, at this point, this work briefly discusses another challenge, i.e., societal challenge [26]. As we have already elaborated various applications of IoT, including numerous societal applications in Section 2, needless to say, that the challenges will follow up with the same enormity.

The primary societal challenge is talent breach. In other words, although the world is moving with a high rapidity towards IoT, still the world is lacking the expert crowd to implement IoT successfully. Mohanty et al. [62] analysed the problem of analysts to review the large-scale data for efficient use. Authors suggested the use of Big Data analytics and algorithm based approached to confront the situation.

Another crucial societal challenge is disapproval of the novel paradigm by masses. Using IoT for various purposes is one of the prime lead of IoT, but its growth is still hampered because it is still not acceptable by people. Asplund and Nadjm-Tehrani [63], conducted a survey based on a set of questions to a group of actors. Authors recorded the general perception and risk perception of masses on IoT. The reasons behind dissatisfaction of end users involve privacy issues, economic issues, or even discomfort towards the adaptation of new technology. Conclusively, establishing confidence among the end users, practitioners have to work very hard and long.

Although "efficient data handling" is a technological challenge, still the same issue arrives here in a different presentation. Different IoT platform uses distinct data management techniques. The motivation behind the use of the diverse data management techniques is frequent innovation in technology, competition in the market, financial issues, and even brand consciousness of varied users [32]. It gives rise to the problem of heterogeneity and lack of interoperability, therefore formulating data-syndication our next prime societal challenge [33, 34].

The excitement around the IoT paradigm and its applications imply that there is a decent competition as well. Companies are progressively alert about the market value of IoT and therefore taking convincing steps towards the adoption of IoT paradigm, making the availability of wide-ranging and extensive technology. However, this is not the only scene, this competition and availability of wide-ranging technology in accordance, poses the next key challenge namely technology selection. It is faced by society whenever to make the best choices out of the available options, along with the least risk adoption.

User-friendliness is also an unavoidable challenge. Finally, practitioners and IoT sponsors have to put up efforts against all these challenges before any IoT system can be made successful for both of them. Mihovska and Sarkar [64], discussed the people-centric smart object connections to facilitate their living. Author's argued the use of information and communication methodologies in smart

assisted living. Bogdan et al. [65] proposed an energy efficient mathematical model for complex IoT systems. The proposed energy efficiency in terms of communicating only essential information among devices while processing the continuous stream of data and metadata.

3.3. Environmental challenges

The effectiveness of technology is directly linked to the enormity of related challenges. As far as IoT is concerned, it is one of the effective paradigms that make the user's life easier to live. After the Internet, cloud computing, mobile computing, and similar paradigms, whose influences were up-to-the information world only, IoT have its impact on the physical world also, definitely comprising information world in it [26]. As the Internet can make an information world much easier to work-in, similarly IoT makes the physical world environment more pleasant to live-in.

The foremost environmental challenge with IoT is power consumption. As computing becomes an inevitable part of each and every aspect of human's life, power consumption becomes an inescapable issue too. Therefore, practitioners have to work on low power consumption by the smart devices being used in IoT implementation. Mihovska and Sarkar [64] advised the use of common platforms to share data among smart devices for low power consumption. Their IoT platform uses low power solutions like solar power.

Another crucial environmental challenge is failure tolerance. As we have already discussed a wide range of applications in earlier sections, the dependency of a human being on computing is quite evident and understandable. This dependency in case of technology failure could lead to tolerable losses (in the case of domestic and societal applications) to unmanageable and wild mishaps (in the case of medical and emergency applications). Jung et al. [66] proposed the use of on-demand remote-code-execution approach and the storage less sensors inefficient way. Authors argued the implementation of static compiled and predefined functionality to enhance the performance of the system. They proposed an IoT framework where a single code is distributed to a unit block with required updating.

Another challenge under consideration is economy and cost. Billions of IoT devices are being used and will be planted in near future to accomplish success. Lee and Lee [67], discussed the challenge of cost-benefit trade-off in the context of huge investments in IoT and uncertain returns. However, up to now, no major solution has been generated to minimize the cost of IoT devices. The cost of an IoT device must be extremely low; therefore, it is rather important to give thoughtful consideration to the economy issues before implementing the technology.

4. Application Domains of IoT

There are different spheres of life where IoT can be applied. The IoT represents a perspective where the Internet has been engrained itself into each and every entity. Here each physical entity (precisely said a thing) is connected to the computing world and can be regulated and coordinated remotely. These objects can also turn up as an access point to communicate with other objects and hence access different internet services. Therefore, due to its presence in each sphere of the physical

world, IoT has been evolved as a paradigm whose implementation can cover a wide variety of application domains. Its tremendous exposure is easily foreseeable in the near future. The outcome of the capability to interconnect the embedded devices with limited CPU, memory and power resources consequently allows the IoT to discover applications in nearly every field [68].

Many academicians and researchers have recognised an extensive range of IoT applications. In 2012, a ranking report [69] was published, that described 50 remarkable application areas of IoT. Finally these application areas were further generalised into 13 sets (i) Smart-cities, (ii) Smart-environment, (iii) Smart-water, (iv) Smart-metering, (v) Security & Emergencies, (vi) Retail, (vii) Logistics, (viii) Industrial control, (ix) Smart-Agriculture, (x) Smart-Animal-farming, (xi) Demotic and Home automation, (xii) Smart-Education and (xiii) e-Health.

According to Perera et al. [70], the IoT application fields can be roughly put into five key categories: smart wearable, smart home, smart city, smart environment, and smart enterprise.

Matta et al. [26] also proposed the classification of application areas into five broader categories. This classification is based on the requirements of the tasks. These categories are: (i) Domestic; (ii) Societal; (iii) Environmental; (iv) Technological; and (v) Emergency and Critical Situations.

These categories can be further discussed under the name of different subcategories, as shown in Fig. 4.

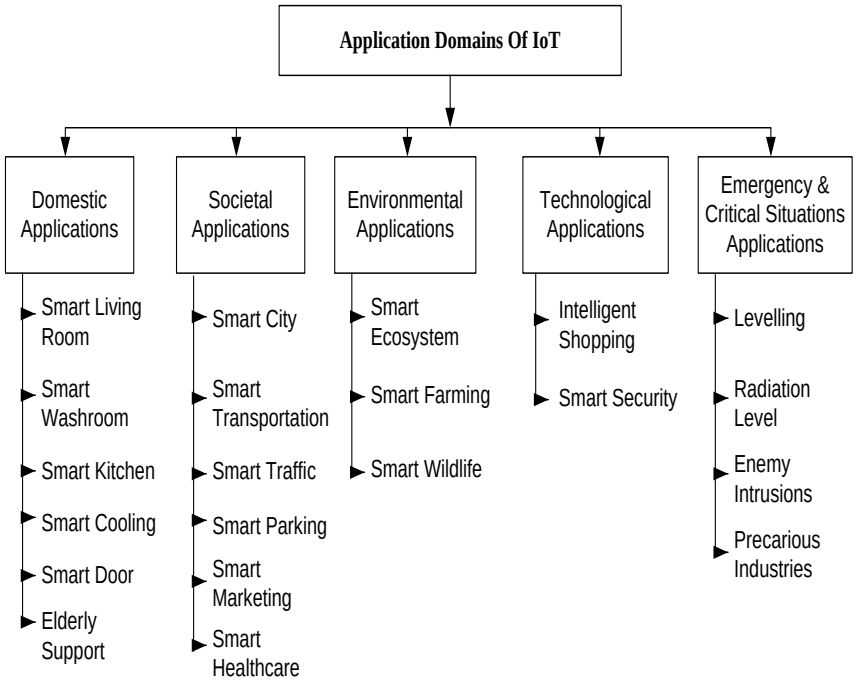

Fig. 4. Application domains of IoT.

4.1. Domestic applications

Domestic applications may include a smart living room, smart washroom, smart kitchen, smart cooling, smart door, and smart elderly support [71, 72].

The smart living room includes the provision of playing the music of guest's choice on their arrival can be implemented. It can be implemented in a way that lights can be dimmed off or completely off on the basis of weather and/or occupancy of the room.

Smart washroom may have the provision of water temperature to be maintained based on weather and person's own likeness. Its applicability can be extended to a warming of water in the tank according to the current season. It can also be designed in a way that in case of any overflow of water or any leakage, required communication and suitable action can be accomplished.

The smart kitchen is one of the major requirements in today's busy life. This category is suitable where all of the persons living in a house are having a busy schedule. In this case, raw food can be kept in a vessel or appropriate cooker, and then it can be controlled remotely so that food can get prepared whenever required. This category also covers the scenario where any unwanted incident like overheating of some edible, or leakage of boiling milk or tea, can occur, and therefore avoid the mishaps. Gas leakage can also be sensed and taken care by implementing the required sensors and alarming devices.

Smart cooling refers to the temperature management of different areas of the house according to the user. The temperature of room, kitchen or even washroom can be regularized on the basis of presence or absence of a person, or even on the basis of a particular person's choice.

The smart door gets open on the arrival of an authenticated person and gets closed accordingly. It can be operated in some other customised manner as if the time is after midnight, the door will also convey the message on the mobile of a specified person. Another provision may be if all the persons living in a house are on a holiday, it can be customized to inform them about even the arrival of an authenticated person in their absence

Smart elderly support comprises of special care of elderly people. The most important and critical routine of everyone's life is to take care of their near and dear ones. Elderly people, as well as children in the house, need special care. They can also get monitored and get assistance if the house is a smart home.

The people living on this earth are continuously ageing. Today the older population (aged 65 and over) represents 7 percent or more of the total population in many parts of the world. In fact, by the mid of this century, 1 billion persons will cross the age of 65 and they can be designated as non-working aged people. Worldwide, the population aged 80 and over is projected to more than triple between 2015 and 2050, from 125 million to 434 million [70]. This mass will require special care to survive and live an improved, secured and reliable life. Therefore, the quality-of-life can be significantly improved by the apropos implementation of IoT. Here, smart wristbands and headbands can be used. These bands have sensors that can sense the chemical present in their sweat and these chemicals are measured and then analysed. The resultant is transmitted to some

device (may be a mobile phone) wirelessly and therefore can help in evaluating and observing the user's health.

4.2. Societal applications

Societal applications may include smart city, smart transportation, smart traffic, smart parking, smart marketing and smart healthcare [71].

Applications focusing on the smart city may include the adaptive streetlight system that can go on or off depending on the weather and level of natural light. It can maintain the garbage levels in garbage containers lying in the city and therefore schedule the trash collection. Another issue covered in such application area is to monitors the sound level raised due to parties, or announcements near schools and hospitals, and in a residential area [73].

In today's life, transportation forms one of the major components of the running busy society, and therefore Smart Transportation gets a high emphasis [73]. The scheduling of routes and time slots can be categorised to heavy-loaded, medium-loaded and under-loaded transportation vehicles. This can be planned and monitored via implementation of IoT system.

Related to smart transportation, one can formulate Smart Traffic. This subcategory is focused majorly on the provision of monitoring the overall traffic management in a city. It includes monitoring the traffic routing within a city, both vehicles as well as pedestrians. This application may also include detection and direction towards the shortest possible route between two points.

Another issue is smart parking that incorporates two basic provisions. The first one entails the system that can monitor the availability of parking space in the city or nearby area. The other is to direct the people towards the available space within a particular parking area.

Smart marketing consists of demand and consumption of various items in the city. It covers the marketing of products on a recommendation basis. It also monitors the demand of a product on the basis of season, i.e., whether it is winter or summer; days, i.e., weekdays or weekends, or it may also be reliant on the festive seasons.

Smart Healthcare is one of the most important societal applications [74]. It may deal with the availability of ambulance from a nearby hospital in a shortest time and it must be assured that ambulance follows the shortest possible route. It comprises of the medication-reminding process, i.e., reminding the schedules of medication to elderly people, or routine medication of children or the persons suffering from long-term diseases [73].

4.3. Environmental applications

Environmental applications may include smart ecosystems, smart farming, smart wildlife and smart water.

Smart ecosystem covers the subjects of quality improvement of air and water. It also deals with noise pollution, especially in residential areas, near hospitals and schools. It includes the provision of environmental monitoring that can resultantly

take care of non-biodegradable garbage. It can also help the authorities to reduce the consumption of polythenes and other non-biodegradable materials by the public.

Smart farming deals with both animal farming and agribusiness in the areas artificially prepared by human beings for husbandry. It may be proved very useful to sense, analyse and monitor a different set of situations related to the animals. It includes climatic conditions, temperature, toxic gas levels, the ratio of animal count to food quantity, number of caretakers and even required fencing around them. On the basis of the analysis, further beneficial and counter actions can be taken [75].

Smart wildlife can be responsible for collecting and analysing information from natural habitats and wildlife ecosystems. This information can become input for the necessary actions for the betterment of the ecosystem. It can also sense the particular case of emergency either related to an animal or a human being in the wildlife area. Applicable signals can be generated; analysed and further appropriate life-saving actions can be taken. This can also be extended to the zoo, resorts and entertainment parks where animals are kept for entertainment and showcasing. Cases of mishap or accidents, either intentional or unintentional can be reported on time, and therefore useful for mankind.

The subcategory of smart water majorly deals with the quality of water. It can check the presence of toxic chemicals, virus or any sort of fungus in water bodies. Required medicated chemicals, insecticides and intoxicants can be added into the water body after the proper analysis and decisions. It can protect water animals as well as water plants in an appreciable manner. It also extends its application in water levelling during summers as well as the rainy season.

4.4. Technological applications

Technological applications may include Intelligent Shopping and Smart Security [76].

Intelligent shopping covers different scenarios like proposing attractive deals to different customers based on their likings and favourite brands. It can be done by keeping the record of the most usual days or dates a customer goes for shopping. By analysing this record and shopping habits, the customer can be traced on his mobile. On recommendation basis, the system can prompt the advertisement of the user's likings on user's Google or Facebook page. Another approach is, by telling the availability as well as reminding the need of products after monitoring and analysing the selection, mode and time gap of his shopping.

Smart security covers security in various ways [77]. It may be the security of documents, things, and equipment in a highly critical scenario like a nuclear power station or defence organisations. It also extends its implementation in a confidential scenario like medical records, law enforcement institutions, and banking sector. Security provision can also be carried out in a routine business sector, typical industrial environments or even in an education sector.

4.5. Emergency and critical situations applications

Emergency and critical situations applications may include natural calamities, water levels, radiation levels, enemy intrusions and precarious industries [78].

The first sub-category covers the possible forecasting of weathers-change, which may lead to some kind of natural calamity, and proceed further accordingly.

Water levelling includes implementation of an IoT system, comprising of sensors, transmitters into a water body. The sensors sense the data, transmits the data to some computing device, where it may be analysed. After analysing the data further directions can be given to authorities dealing the water level problems.

Similarly, radiation levels can be monitored in radiation generating vicinities. these vicinities may range from a least critical microwave oven to the most critical nuclear plant, where the minute changes in the radiation levels can bring a hazard.

Enemy intrusions is another foremost issue in various parts of the world. On the borders, by implementing sensors and cameras, one can prevent or take appropriate actions for unwanted intrusions.

Precarious industries form application area under the emergency and critical situations applications. This category covers the industries where extra precaution is required to be safe and secure. Industrial areas like fireworks, coal mine, tunnels, and dams are also life-threatening points; therefore an efficient and robust IoT implementation can be applied in these areas to avoid the disasters at the public level or mishaps at the individual level.

5. Conclusion

After observing the driving force of enormous applications of IoT, it is quite evident that the paradigm of IoT will make its own way into the marketplace over the coming years. Further, we can see a significant number of open challenges and therefore can focus to generate the new solutions or strengthen the already existing solutions for these challenges. Moreover, we also see a plentiful of aspects be considered when talking about IoT and its effectiveness. The aspects may be increased efficiency, architectures supporting interoperability, homogeneity in foreground although there is heterogeneity in the background, collecting and mining the related data, the security of data, improved scalability of the system, enhanced concurrency in the entire system.

As far as challenges are concerned, the architecture for such a huge, distributed and heterogeneous environment is the foremost challenge. Another representative challenge is the scalability of the system, its openness and support to highly scalable systems in all the three ways, i.e., geographical, technological as well as magnitudinal. Security and privacy from the viewpoints of both the providers as well as users are other interesting challenges to accept. Edge technologies, like sensors, actuators, RFID are next domain to form the challenge for researchers. Although Big Data and IoT are two different domains, due to the intense and mutual relationship, they overlap each other at a major subject namely, data. And consequently, processing, transforming and analysing the enormous amount of data is next open challenge in both the domains.

Some contributions are already made by some researchers, but still, there are much more to achieve. In near future, to improve the living style and standard of the consumer, everything, every aspect of consumer's life, will be "smart", and therefore we have to look forward to more interesting, efficient, effective and novel solutions for IoT paradigm. Hence, IoT and its efficient implementation require

direct attention towards research. Moreover, the world looks forward to an ample amount of investment to be made in research and development towards the solutions and technologies supporting IoT. These solutions are intended to make our life "smart" life and therefore our world "smart" world.

This paper mainly elaborates the solutions given by distinguished researchers in the field of IoT in the current scenario and therefore provides a comprehensive reference source for the researchers involved in this field.

References

1. International Telecommunication Union (ITU). (2015). Internet of things global standards initiative. Retrieved January 8, 2017, from http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.
2. China Communication Standards Association. (2011). [YDB] Communication standard technical report. Retrieved March 20, 2017, from http://www.ccsa.org.cn/english/list_std.php?tbname=ydb_doc&keyword=&page_currentPage=4.
3. International Telecommunication Union (ITU). (2012). Y.2060: Overview of IoT. Retrieved January 15, 2017, from https://www.itu.int/rec/T-REC-Y.2060-201206-I.
4. Vermesan, O.; Friess, P.; Guillemin, P.; Gusmeroli, S.; Sundmaeker, H.; Bassi, A.; Jubert, I.S.; Mazura, M.; Harrison, M.; Eisenhauer, M.; and Doody, P. (2011). Internet of things strategic research roadmap. *Internet of Things – Global Technological and Societal Trends*, 9-52.
5. Lee, G.M.; Park, J.; Kong, N.; and Crespi, N. (2012). The internet of things - concept and problem statement. *Internet Research Task Force*, 19 pages.
6. Yan, L.; Zhang, Y.; Yang, L.T.; and Ning, H. (2008). *Internet of things: From RFID to the next-generation pervasive networked systems* (1st ed.). Boca Raton, Florida: Auerbach Publications.
7. Chen, S.; Xu, H.; Liu, D.; Hu, B.; and Wang, H. (2014). A vision of IoT: Applications, challenges, opportunities with China perspective. *IEEE Internet of Things Journal*, 1(4), 349-359.
8. Hendricks, D. (2015). The trouble with the internet of things. Retrieved December 24, 2016, from http://data.london.gov.uk/blog/the-trouble-with-the-internet-of-things/.
9. International Telecommunication Union (ITU). (2005): The internet of things. ITU internet report. Retrieved January 10, 2017, from https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf.
10. Europen Research Cluster (IERC). (2014). Internet of things. Retrieved March 21, 2017, from http://www.internet-of-things-research.eu/about_iot.htm.
11. Santucci, G. (2010). The internet of things: Between the revolution of the internet and the metamorphosis of objects. *Vision and challenges of realising the Internet of Things*, 11-24.
12. Evans, D. (2011). *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*. San Jose, California, United States of America: Cisco.

13. Kosmatos, E.A.; Tselikas, N.D.; and Boucouvalas, A.C. (2011). Integrating RFIDs and smart Objects into a unified internet of things architecture. *Advances in Internet of Things*, 1(1), 5-12.
14. National Intelligence Council. (2008). Disruptive civil technologies. Six technologies with potential impacts on the US interests out to 2025. Retrieved April 22, 2017, from https://fas.org/irp/nic/disruptive.pdf.
15. Tsai, C.-W.; Lai, C.-F.; and Vasilakos, A.V. (2014). Future internet of things: Open issues and challenges. *Wireless Networks*, 20(8), 2201-2217.
16. Wan, J.; Yan, H.; Suo, H.; and Li, F. (2011). Advances in cyber-physical systems research. *KSII Transactions on Internet and Information Systems*, 5(11), 1891-1908.
17. Hachem, S.; Teixeira, T.; and Issarny, V. (2011). Ontologies for the internet of things. *Proceedings of the 12th International Middleware Conference.* Lisbon, Portugal, 6 pages.
18. Dobre, C.; and Xhafa, F. (2014). Intelligent services for big data science. Future *Generation Computer Systems*, 37, 267-281.
19. Sundmaeker, H.; Guillemin, P.; Friess, P.; and Woelffle, S. (2010). *Vision and challenges for realising the internet of things*. (CERP-IoT) Cluster of European Research Projects on the Internet of Things. Brussels, Belgium: European Commission.
20. Gartner. (2013). Gartner says the internet of things installed base will grow to 26 billion units by 2020. Retrieved from January 20, 2017, from https://attivonetworks.com/gartner-says-the-internet-of-things-installed-base-will-grow-to
-26-billion-units-by-2020/.
21. ABI Research. (2013). More than 30 billion devices will wirelessly connect to the internet of everything in 2020. Retrieved March 20, 2017, from https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/.
22. Anderson, J.; and Raine, L. (2014). Main report: An in-depth look at expert responses. Retrieved December 12, 2016, from http://www.pewinternet.org /2014/05/14/main-report-an-in-depth-look-at-expert-responses/.
23. HM Treasury and Osborne , G. (2015). Budget 2015: Some of the things we've announced. Retrieved March 31, 2016, from https://www.gov.uk/ government/news/budget-2015-some-of-the-things-weve-announced.
24. Arseni, S.-C.; Halunga, S.; Fratu, O.; Vulpe, A.; and Suciu, G. (2015). Analysis of the security solutions implemented in current Internet of Things platforms. *Proceedings of IEEE International Conference on Grid, Cloud and High Performance Computing in Science (ROLCG).* Cluj-Napoca, Romania, 1-4.
25. Miorandi, D.; Sicari, S.; De Pellegrini, F.; and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497-1516.
26. Matta, P.; Pant, B.; and Arora, M. (2017). All you want to know about internet of things (IoT). *Proceedings of 4th IEEE International Conference on Computing, Communication and Automation (ICCCA).Greater Noida,* India, 1306-1311.

27. Castellani, A.P.; Bui, N.; Casari, P.; Rossi, M.; Shelby, Z.; and Zorzi, M. (2010). Architecture and protocols for the Internet of Things: A case study. *Proceedings of 8th IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM). Mainheim, Germany*, 678-683.
28. Beier, S.; Grandison, T.; Kailing, K.; and Rantzau, R.(2006). Discovery services - enabling RFID traceability in EPCglobal networks. *Proceedings of the 13th International Conference on Management of Data (COMAD)*, 4 pages.
29. Gronbaek, I. (2008). Architecture for the Internet of Things (IoT): API and interconnect. *Proceedings of 2nd International Conference on Sensor Technologies and Applications (SENSORCOMM).* Cap Casterel, France, 802-807.
30. Dai, G.; and Wang, Y. (2012). Design on architecture of Internet of Things. *Advances in Computer Science and Information Engineering*, 1-7.
31. Tan L.; and Wang, N. (2010). Future internet: The Internet of Things. *Proceedings of 3rd International Conference on Advanced Computing Theory Engineering (ICACTE).Chengdu, China,* 5, 376-380.
32. Ma, H.-D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer Science and Technology*. 26, 919-924.
33. Bandyopadhyay, D.; and Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), 49-69.
34. Sarkar, C.; Nambi, A.U.S.N. ; Prasad, R.V.; Rahim, A.; Neisse, R. and Baldini, G. (2015). DIAT: A scalable distributed architecture for IoT. I*nternet of Things Journal*, 2(3), 230-239.
35. Ning, H.; and Wang, Z. (2011). Future Internet of Things architecture: Like mankind neural system or social organization framework? *IEEE Communications Letter*, 15(4), 461-463.
36. Kovatsch, M.; Mayer, S.; and Ostermaier, B. (2012). Moving application logic from the firmware to the cloud: Towards the thin server architecture for the Internet of Things. *Proceedings of 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS).* Palermo, Italy, 751-756.
37. Baraniuk, R.G. (2011). More is less: Signal processing and the data deluge. *Science*, 331*(*6018), 717-719.
38. Waldner, J.-B. (2013). *Nanocomputers and swarm intelligence*. Hoboken, New Jersey: John Wiley & Sons, Inc.
39. Zhang, J.; and Sun, Y. (2012). Managing resources in Internet of Things with Semantic hyper-network model. *Proceedings of the International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*. Hammamet, Tunisia, 318-323.
40. Lopez, T.S.; Brintrup, A.; Isenberg, M.-A.; and Mansfeld, J. (2011). Resource management in the Internet of Things: Clustering, synchronisation and software agents. *Architecting the Internet of Things*, 159-193.
41. Helsinger, A.; Thome, M.; and Wright, T. (2014). Cougaar: A scalable, distributed multi-agent architecture. *Proceedings of IEEE International Conference on Systems, Man and Cybernetics.* The Hague, Netherlands, Volume, 2, 1910-1917.

42. Lopez, T.S.; Ranasinghe, D.C.; Harrison, M.; and McFarlane, D. (2012). Adding sense to the internet of things. *Personal and Ubiquitous Computing*, 16(3), 291-308.
43. Yu, R.; Zhang, Y.; Gjessing, S.; Xia, W.; and Yang, K. (2013). Toward cloud-based vehicular networks with efficient resource management. *IEEE Network*, 27(5), 48-55.
44. Stankovic, J.A. (2014). Research directions for the internet of things. IEEE *Internet of Things Journal*, 1(1), 3-9.
45. Kawamoto, Y.; Nishiyama, H.; Kato, N.; Shimizu, Y.; Takahara, A.; and Jiang, T. (2015). Effectively collecting data for the location-based authentication in Internet of Things. *IEEE Systems Journal*, 11(3), 1403-1411.
46. Tsai, C.-W.; Lai, C.-F.; Chiang, M.-C.; and Yang, L.T.(2014). Data mining for internet of things: A survey. *IEEE Communications Surveys and Tutorials*, 16(1), 77-97.
47. Farooq, M.U.; Waseem, M.; Khairi, A.; and Mazhar, S. (2015). A critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications*, 111(7), 6 pages.
48. Machara, S.; Chabridon, S.; and Taconet, C. (2013). Trust-based context contract models for the internet of things. *Proceedings of IEEE 10th International Conference on Ubiquitous Intelligence and Computing and IEEE 10th International Conference on Autonomic and Trusted Computing*. Vietri sul Mere, Italy, 557-562.
49. Matta, P.; Pant, B.; and Tiwari, U.K. (2017). DDITA: A naive security model for IoT resource security. *Smart Innovations in Communication in Computational Science*, 199-209.
50. Fazio, M.; Celesti, A.; Puliafito, A.; and Villari, M. (2014). An integrated system for advanced multi-risk management based on cloud for IoT. *Advances onto the Internet of Things: How Ontologies Make the Internet of Things Meaningful*, 253-269.
51. Hardy, Q. (2017). Tim O'Reilly explains the Internet of Things. Retrieved February 25, 2019, from https://bits.blogs.nytimes.com/2015/02/04/tim-oreilly-explains-the-internet-of-things/
52. Aggarwal, R. and Das, M.L. (2012). RFID security in the context of "internet of things". *Proceedings of First International Conference on Security of Internet of Things.* New York, United States of America, 51-56.
53. Cardwell, D. (2014). At Newark Airport, the lights are on, and they're watching you. *The New York Times*.
54. Perera, C.; Ranjan, R.; Wang, L.; Khan, S.U.; and Zomaya, A.Y. (2015). Privacy of big data in the Internet of Things era. *IEEE IT Professional Magazine*, 17, 32-39.
55. Yoshigoe, K.; Dai, W.; Abramson, M.; and Jacobs, A. (2014). Overcoming invasion of privacy in smart home environment with synthetic packet injection. *Proceedings of the TRON Symposium (TRONSHOW). Tokyo, Japan*, 1-7.
56. Steinberg, J. (2014). These devices may be spying on you (even in your own home). Retrieved April 2, 2017, from http://www.forbes.com/sites

/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/#3be3cba66376.

57. Vylegzhanina, V.; Schmidt, D.C.; and White, J. (2015). Gaps and future directions in mobile security research. *Proceedings of 3rd International Workshop on Mobile Development Lifecycle*. New York, United States of America, 49-50.
58. Kim, J.y. (2015). Secure and efficient management architecture for the Internet of Things. *Proceedings of 13th ACM Conference on Embedded Networked Sensor Systems (SenSys).* New York, United States of America, 499-500.
59. Jing, Q.; Vasilakos, A.V.; Wan, J.; and Lu, J.; and Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*, Springer, 20(8), 2481-2501.
60. Barreto, L.; Celesti, A.; Villari, M.; Fazio, M.; and Puliafito, A. (2015). An authentication model for IoT Clouds. *Proceedings of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. Paris, France, 1032-1035.
61. Mansfield-Devine, S. (2015). The dangers lurking in smart buildings. Computer *Fraud and Security*, 2015(11), 15-18.
62. Mohanty, S.; Das, S.K.; Barik, S.; and Rout, M.M. (2016). A survey on big data and its challenges related to IoT. *Proceedings of International Interdisciplinary Conference on Engineering Science and Management.* Goa, India, 331-334.
63. Asplund, M.; and Nadjm-Tehrani, S. (2016). Attitudes and perceptions of IoT security in critical societal services. *Special Section on the Plethora of Research In Internet Of Things (IoT)*, 4, 2130-2138.
64. Mihovska, A.; and Sarkar, M. (2018). Smart connectivity for Internet of Things (IoT) applications. *New Advances in the Internet of Things*, 105-118.
65. Bogdan, P.; Pajic, M.; Pande, P.P.; and Raghunathan, V. (2016). Making the Internet-of-Things a reality: From smart models, sensing and actuation to energy-efficient architectures. *Proceedings of the International Conference on Hardware/Software Codeware and System Synthesis* (*CODES/ISSS).* Pittsburgh, Pennsylvania, United States of America, 1-10.
66. Jung, M.; Park, D.; and Cho, J. (2015). Efficient remote software execution architecture based on dynamic address translation for Internet-of-Things software execution platform. *Proceedings of 18th IEEE International Conference on Network-Based Information Systems.* Taipei, Taiwan, 371-378.
67. Lee, I.; and Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizon*, 58(4), 431-440.
68. Vongsingthong, S.; and Smanchat, S. (2014). Internet of Things: A review of applications and technologies. *Suranaree Journal of Science and Technology*, 21(4), 359-374.
69. INFSO D.4 Networked Enterprise, RFID INFSO G.2 Micro and Nanosystems; and Working Group RFID ETP EPoSS. (2008). *Internet of Things* in *2020: Roadmap for the future*. Version 1.1. Brussels, Belgium: European Commission.

70. Perera, C.; Liu, C.H.; and Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. *IEEE Transactions on Emerging Topics in Computing*, 3(4), 585-598.
71. Kraijak, S.; and Tuwanut, P. (2015). A survey on Internet Of Things Architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. *Proceedings of 11th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM).* Shanghai, China, 26-31.
72. Perumal, T.; Sulaiman, M.N.; Mustapha, N.; Shahi, A.; and Thinaharan, R. (2014). Proactive architecture for Internet of Things (IoTs) management in smart homes. *Proceedings of the IEEE 3rd Global Conference on Consumer Electronics (GCCE).* Tokyo, Japan, 16-17.
73. Jalali, R.; El-khatib, K.; and McGregor, C. (2015). Smart city architecture for community level services through the Internet of Things. *Proceedings of* 18th *International Conference on Intelligence in Next Generation Networks*. Paris, France, 108-113.
74. Hassanalieragh, M.; Page, A.; Soyata, T.; Sharma, G.; Aktas, M.; Mateos, G.; Kantarci, B.; and Andreescu, S. (2015). Health monitoring and management Using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. *Proceedings of IEEE International Conference on Services Computing*. New York, United States of America, 285-292.
75. Lin, Z.; Hu, H.; Zhang, Y.; Qiao, J.; and Xue, J. (2011). The application of the internet of things in agriculture. *Applied Mechanics and Materials*, 687-691, 2395-2398.
76. Bing, K.; Fu, L.; Zhuo, Y.; and Yanlei, L. (2011). Design of an internet of things-based smart home system. *Proceedings of 2nd International Conference on Intelligent Control and Information Processing*. Harbin, China, 921-924.
77. Matta, P.; and Pant, B. (2018). TCpC: A graphical password scheme ensuring authentication for IoT resources. *International Journal of Information Technology*, 1-11.
78. Balampanis, S.; Sotiriadis, S.; and Petrakis, E.G.M. (2016). Internet of Things architecture for enhanced living environments. *IEEE Cloud Computing*, 3(6), 28-34.

Appendix A

Categories and Sub-Categories of Challenges in IoT

Research challenges	Sub-challenges	References	Contribution	Technologies/ architecture used
Technological challenges	**Architecture and heterogeneity**	Castellani et al. [27]	• **Technological challenges**	Architecture and heterogeneity •
		Beier et al. [28]	• Use the concept of discovery services. • Discovery service consists of a well-defined database and a collection of web service interfaces.	• EPC (Electronic Product Code) global IoT architecture • Object-name service
		Gronbaek [29] and Dai and Wang [30]	• Suggests OSI-model like architecture. • Ubiquitous services on an end-to-end basis	• Things layer • Adaptation layer • Internet layer • Application layer
		Tan and Wang [31]	• Layered architecture for the IoT • Authors described five layers	• Application layer • Middleware layer • Coordination backbone layer • Access layer • Edge technology layer
		Ma [32]	• Considered viewpoints of users, developers, service providers and the network providers. • Interfaces, supporting protocols and required standards are defined	• Object sensing layer • Data exchange layer • Information integration layer • Application service layer
		Bandyopadhyay and Sen [33]	• All-purpose layered architecture to represent an IoT system	• Edge technology layer • Access gateway layer • Internet layer • Middleware layer • Application layer
		Ning and Wang [35]	• IoT architectures on the basis of Human neural system and SOF • Proposed two models for IoT architecture namely i) Unit IoT, and ii) Ubiquitous IoT	• M & DC (Management and Centralized Data Centre) resembling the brain • DCN (Distributed Control Nodes) resembling the spinal cord • NoS (Networks and Sensors) resembling nerves

	Kovatsch et al. [36]	• Offered centralised architecture to segregate the device heterogeneity from application development • They proposed the concept of a thin server	• Web-like layer • Enhanced server
	Hendricks [8], Baraniuk [37], and Waldner [38]	• Scalability through usage of the internet completely • More prone to the vast range of adversaries	• Network device • Network topologies • Network configuration • Various forms of data representation, • IPv6 addressing scheme
Resource management	Zhang and Sun [39]	• Offered a model named Semantic hyper-network model to manage and organize the different resources for an IoT system. • Semantic hyper-network is offered as SHN = (N, L).	• Used hypergraphs to show resources and their relations • All the resources are represented by vertices and similarly, edges are used to represent their relationships • Defined 6 operations on Hypergraphs
	Helsinger et al. [41]	• Suggested use of software agents • Proposed Cougaar as a scalable and distributed multi-agent architecture to support resource management • A plug-in is described as a software module that forms the application logic, to be added into an agent	• Cougaar component model • Plugins • Message transport service • Blackboard • Persistence • Naming service • Community • Service discovery • Servlets and logical domain model
	Lopez et al. [42]	• Proposed smart object framework • This framework is capable of identifying and monitoring the status of things, and therefore, the structure of the network is decided accordingly	• Radio-Frequency Identification (RFID) • Sensor technologies, object ad-hoc Network • Embedded object logic • Internet-based information Infrastructure

	Yu et al. [43]	• Proposed a specific architecture for a specific IoT application • Proposed the use of cloud architecture for the smart vehicular networks • They rely on the concept of sharing the resources	• The vehicular cloud • Roadside cloud • Central cloud • Game-theoretical approach
Efficient data handling	Ma [32]	• Proposed "data exchange among large-scale heterogeneous network elements" • Offered the view that it is very critical to handle the exchange of data within a vast heterogeneous network	• Heterogeneous network • Non-uniform data • Inconsistency of data • Inaccuracy of data
	Kawamoto et al. [45]	• They proposed cyclic fashion to collect the data from a limited number of devices • Discussed the authentication model.	• Data collection, • Computer assisted mass appraisal/ CAMA based data collection model
	Tsai et al. [46]	• Emphasised on data mining • They suggested three primary areas of attention: Objective, characteristics of data, and mining algorithm	• Knowledge Discovery in Data (KDD) bases
	Farooq et al. [47]	• Emphasised on data collection • Data used to flow among the devices	• Devices to collect data • Prevailing technologies
Security and privacy	Machara et al. [48]	• Recognized privacy as one of the fundamental subjects • Identified 4 dimensions of privacy - purpose, visibility, retention, granularity	• Data use, • Access data • Times period • Delivery of data
	Matta et al. [49]	• Propose a naive security • Model, namely DDITA • Classified data as private • Data and public data • Stored data is proposed keeping	• Access policy • Resource recognition • Resource valuation • Threat recognition • Access declaration • Privilege definition • Encryption

			encryption authorisation • Authentication, attestation • Encryption using TPM	• Data attestation
		Tsai et al. [15]	Suggested that privacy and security are two upcoming research issues in the paradigm of IoT	Generalised architecture
		Kim [58]	• Suggested architecture to fulfil the purpose of IoT security • Layered architecture including-perception layer, transportation layer, application layer, support layer	• Secure and efficient code dissemination protocol • Reliable and secure multicast protocol • RFID security and WSNs security
		Jing et al. [59]	Suggested three-layer security architecture	• Segmental and sectional security
		Kawamoto et.al. [45]	Discussed authentication in terms of location-based authentication	• Data collection • Data quantity • Ownership of devices
		Barreto et al. [60]	• Proposed an authentication model for IoT • This model categorise the user's request into two categories - direct access to the IoT services, and access to the IoT services	• Cloud provider • Categorisation of users
Societal challenges	Talent breach	Mohanty et al. [62]	• Proposed the use of big data to analyse the data instead of guessing or| conventional methods	• Heterogeneity • Scale • Big data functions
	Disapproval of the novel paradigm by masses	Asplund and Najm-Tehrani [63]	• Survey on the perception of people • Identify information regarding challenges in IoT • Work is referred to as Critical Societal Services (CSS)	• Questionnaire • Actors • Dependencies • Drivers • Enablers
	User-friendliness	Mihovska and Sarkar [64]	• Discussed smart connectivity in AAL scenario • Developed scenarios for the use of efficient protocols and interfaces	• Sensing • Data collection • Data exchange • Data processing • Data storage

Environmental challenges	Power consumption	Mihovska. and Sarkar [64]	• Proposed the feature of low-power consumption to enhance the performance of application • Suggested the transfer of data among devices on a common platform	• Latency • Novel battery approach • Common platform for sensor data
		Bogdan et al. [65]	• Mathematical model for complex systems • Sharing of only essential data and properties • Harvesting of energy through different sources	• Energy harvesting for efficient energy supply • Use of photovoltaics • Thermoelectric generators
	Failure tolerance	Jung et al. [66]	• Applied the theory of remote-on-demand execution • Implemented the storage-less sensor • Distribution of single code to a unit block	• Middleware layer • Energy consumption • Reliable packet delivery
	Economy and cost	Lee and Lee [67]	• Argued the high investment costs and uncertain benefits of IoT • Discusses the higher productivity at lower costs	• Semi-passive RFID • Smart grid • Smart metering