Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 3, May : 2023

IoT, AN ENABLING TECHNOLOGY SURVEY WITH RECENT ISSUES AND CHALLENGES

Ruchi Bhatnagar, Department of Computer Science and Applications, IIMT University, Meerut, India.
Dr. K.K. Sharma, Department of Computer Science and Applications, IIMT University, Meerut, India.

Abstract
Technologies are sprawling with additions to IoT. It has emerged as an area of unbelievable potential and growth of new infrastructure and technology. It becomes a boon for humanity with lot of advantages and are trying to empower the inanimate physical objects to act without any human intervention; Its centric concepts like augmented reality, Smart city, self-driven cars, smart environment, e-health care, etc. have a ubiquitous presence now. While these applications require higher data-rates, large bandwidth, increased capacity, low latency and high throughput. In light of these emerging concepts, this chapter review the enabling technologies of IoT that makes possible to predict futuristic techniques. It also shed light on concerned issues and challenges faced by these enabling technologies with their perspective solutions. Furthermore, it focuses on art of current state and future research directions of IoT.

Keywords: Internet of Things(IoT), Wireless Sensor Network(WSN), Big Data Analytics, Green Computing, Software Defined Networking

1. Introduction

This Internet of Things or IoT has originating a new revolutionary world from smart refrigerator to wearable technologies and from smart homes to smart conurbation soon [1]. It is an emerging model that enables the communication based on IP between electronic devices and sensors through the internet in order to facilitate our lives [2]. Now it becomes an important aspect of our life that can be sensed everywhere around us. IoT is an invention that puts together wide variety of smart systems, frameworks and intelligent devices and sensors. Moreover, it takes advantage of quantum and nanotechnology in terms of storage, Green computing in terms of environment, processing speed in terms of 5G and which were not conceivable earlier [3]. The objectives of IoT is not just allowing billions of devices communicate simultaneously but also taking business decision making and automating diverse processes. It also helps to overcome many challenges, through increased capacity and Artificial intelligence and enhancing a new web era.

The term IoT was devised by Kevin Ashton in 1999 with reference to the supply chain management [4]. The concept of IoT means ‘‘smartness’’ – ‘‘an ability to independently obtain and apply knowledge’’ [5]. Consequently, IoT refers to the ‘‘things or devices and sensors’’ that are smart, uniquely addressable based on their communication protocols, and are adaptable and autonomous with inherent security. Atzori et al. [6] have characterized IoT in three visions. The first one is Internet Oriented vision i.e. the vision focusses on connectivity between the things; second is things Oriented that means the vision focusses on generic objects; and the third one is Knowledge Oriented that elaborates the vision focusses on how to represent, store and organize information. These visions paved towards International Telecommunication Union (ITU) vision of IoT, which states it as ‘‘anytime, anyplace connectivity for anyone’’ [7]. In a nutshell, the ultimate objective is of IoT is ‘‘to plug and play smart objects’’. The basic IoT layout is comprises by connected devices, central control hardware, data cloud, user interface and network interconnection but the complementary advancements in underlying hardware and software technologies led to the explosive growth of this infrastructure with new technologies.

IoT is enabled by several technologies including wireless sensor networks, cloud computing, Big data analytics, Embedded Systems, Security Protocols and architectures, communication protocols, fifth generation (5G) networks and Semantic Search engines. Using these technologies, the 'smart environment' concept has become boom but diverse as it covers transportation/logistics, healthcare, utilities, personal home/offices and much more. In the IoT decade, concepts like augmented maps, autonomous car, mobile ticketing, and passenger counting in transportation/logistics domain have been successfully implemented; while the continuous improvement in these technologies is also currently in practice.

The objectives of this chapter focuses on:

1. Provides an overview of technical details of each technology associated with IoT.
2. Summary of key IoT issues and challenges presented in the recent literature.
3. Brief support of literature by reviewing it.
4. To understand the need for integration of different application areas with new technologies.
5. The future research directions for researchers and practitioners.

The remaining part of paper has been organized as follows: section 2 briefs the IoT enabled Technologies; section 3 elaborates related issues and challenges faced by each enabling technology; section 4 has proposed future research directions and section 5 conclude the survey paper.

2. IoT Enabled Technologies

IoT provides a new paradigm with set of new services for the next wave of technological innovations. Its applications are nearly limitless while enabling different technology and their seamless integration with the physical world made IoT a high demand network. Enabling technologies for the Internet of Things are grouped into three categories i.e. technologies that enable "things" to attain contextual information, technologies that permit "things" to process contextual information, and [8] technologies to improve safety and privacy of the network. The first two categories make functional building blocks of IoT i.e. "intelligence" into "things"; It also made functional features of IoT that differentiate it from the usual Internet. While the third category is not a functional but rather a factual requirement, without which the penetration of the IoT would be severely reduced [9]. The brief introduction of these enabling technologies that affords the users of IoT to use these extensive techniques are:

2.1. Wireless Sensor Network

The common vision of smart grid, smart homes, intelligent transportation and other infrastructure systems is usually associated with one single concept, the internet of things (IoT), where through the use of sensors, the entire physical infrastructure is closely coupled with information and communication technologies and intelligent monitoring and management can be achieved via the usage of networked embedded devices. WSNs are collection of spatially dispersed and dedicated sensors for monitoring and recording to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT. A wireless sensor network (WSN) is the leading component of IoT that folds surrounding information and sends it to the main server for its execution represented in Figure 1. However, unlike traditional WSN, IoT-based WSN needs to be smarter [10]. Predominantly, IoT-based WSN does not only execute ordinary tasks, for instance, collecting environmental data, but also perform important functions with least or no human involvement. It is now combined with IoT in an innovative way to moving towards new technology.

2.2. Cloud Computing

IoT is not just provide functions of systems connectivity, data collection, their storage, and analytics alone but also helps in streamlining the operations by connecting the legacy and smart devices,

machines to the internet, and reducing the hurdles between IT and operations with a unified view of the systems and data. However, with the amount of big data that is generated by IoT, a lot of strain is put on the internet infrastructure. This has made users to look for an option that would reduce this load. The integration of cloud computing gives these opportunities to an IoT. The on-demand delivery of computing power, database storage, applications and IT resources facilitates multiple customers with the help of a multi-tenant cloud model. It enables organizations to provide high level abstraction like a virtual machine (VM) infrastructure at user premises instead of building a computing infrastructure. Cloud computing, as well as IoT, work towards increasing the efficiency of everyday tasks and both have a complementary relationship. On one hand, IoT generates lots of data while on the other hand, cloud computing overlays way for this data to travel. Cloud computing also enables enterprises to scale up the infrastructure, depending on their needs, without setting up an additional hardware and infrastructure. In addition to this, cloud computing also enables better collaboration for users by facilitating to store as well as access data remotely. Thus has altered the way in which technologies can be accessed, managed and delivered and act as important utility services in the future [11].

2.3. Big Data Analytics

As the large amount of data generated by IoT dealing with their storage and analytics facilitates data-driven decisions that can improve business-related outcomes. It has exponentially increased over the time and promise competitive advantages in Business. As a result, the demands of adapting data analytics to big data in IoT have increased as well, thereby changing the way that data are collected, stored, and analyzed. Big data and analytics have great potential for extracting meaningful information from the data produced by sensor devices [12]. The data that may store in many different platforms used to filter, aggregate and analyses by stream analytics [13] and make data integration process becomes vital. The big data enabling technologies in the IoT context are related to ubiquitous wireless communication, real-time analytics, machine learning, and data capturing elements, such as commodity sensors and embedded systems. Big data technologies can also be offer data storage and processing services in an IoT environment, while data analytics allow business people to make better decisions. IoT applications are the major sources of big data.

2.4. Embedded System

The invention of smart devices makes number of task for the person easier. The smart devices are created using embedded systems. Embedded systems are the microprocessor based hardware and software devices that allow the sensor devices to work in a collaborative manner to create an electronic system. These systems are highly customized and programmed as per need of users; follow firmware programming embedded in the micro-chip and stored in read-only memory or flash memory chips. Embedded systems connect with the outside world through peripherals, linking input and output devices [14]. Embedded systems also plays an important role in Internet of Things (IoT) due to their unique characteristics and features such as real time computing, low power consumption, low maintenance and high availability. Numerous embedded systems are around us in the form of commercial systems like vending machines, smart kiosks, AC controller, connected cars, hotel bill printers, etc., which are capable of performing a unique variety of operations. Hence, when it comes to designing of these embedded IoT systems, they need to be designed for specific functions, possessing qualities of a good product design like low power consumption, secured architecture, reliable processor, etc. Real Time Operating System (RTOS), microprocessors and microcontrollers are major players in embedded system hardware and software developments in case of IoT that requires changing current embedded system design and architecture to suit real-time operations, smaller size of the unit and lowered power consumption and become cost efficient for IoT. Use of microcontroller and technologies such as Systems on Chip (SoC) and Reduced Instruction set Computing Chips (RISC) will have greater scope in the field of IoT.

2.5. Security Protocol and Architecture

IoT also termed as cyber-physical system for evaluating state information and performing automatic computation by combining networking infrastructure with smart devices. So that whenever address a security paradigm in IoT a wider aspect of scenarios considers by combining architectures, users, communications, technologies and applications. In an IoT infrastructure nodes are communicating and disseminating information for a short period of time, and sometimes only once in their lifetime. So that its challenging to predict, in advance, which node will interact to which node through which protocol or service through which they will attempt access. To ensuring the security and privacy of the system IoT faced lots of hurdle in form of issues arising during connection to communication. Thus, in highly scalable and dynamic system of IoT, the entity authentication is not only based on single identity but also based on group of identities i.e. 'attributes' that can help to reduce the overhead on the system by avoiding the need to store and specify policies based on the identity of each entity [15]. IoT requires a systematic approach for addressing IoT security issues and challenges and requires a framework build a secure IoT structural design.

2.6. Communication Protocol

Internet of Things (IoT) is a heterogeneous network approach that provides connectivity to the Internet via smart sensing devices to attain identification and management. It provides communication with each other locally and via internet globally. Such kind of network poses several challenges and requirements for choosing the best amongst the available communication technologies [16]. The major communication technologies that can be utilized by IoT devices are summarized below:

i) ZigBee

ZigBee is IEEE 802.15.4 standard. It is reliable wireless networking technology which developed by ZigBee Alliance. It is designed for limited range network monitoring and controlling due to its low data rate and short range. The main area of utilization of this technology is in Home Automation, Smart Energy devices, lighting, HVAC and security etc. Due to its low-power, high level communication protocol using small digital radios, it comes under wireless personal area network (WPAN). It also has a unique functionality of self-organizing, multi-hop and reliable mesh networking with long battery life time [17-19].

ii) RFID

Another preference to connect devices and make them talk is utilize simple radio frequency (RF) boundaries. It can provide communication range between 100m and 1km (depending on the transmission power and the antenna used). RF communication modules do not provide any implementation of the TCP/IP communication protocol (or any other protocol). Data rates are quite low (up to 1Mpbs) and also need an Internet-enabled gateway that will provide access to the devices for making a complete IoT network. The Radio Frequency Identification (RFID) technology has been initially introduced for identifying and tracking objects with the help of small electronic chips, called tags. RFID has been originally categorized as the enabling communication power for the Internet of Things, due to its low cost, high mobility and efficiency in identifying devices and objects. Despite RFID is very common for device identification and some information exchange [20].

iii) Bluetooth

Bluetooth is an IEEE 802.15.1 standard for low cost, short range and cheap devices of wireless radio technology. Bluetooth has been one of the first wireless communication protocols designed with lower power consumption for replacing short-range wired communications (in computer peripherals, mobile phone accessories, etc.), short distance data sharing and devices' mobility support. It has an exceptional property of creating personal area network during communication and discovers and communicates to its neighbor without need to be in visual line of sight. Due to

its global standard it is also known as WPAN (Wireless Personal Area Network). It is very important for the case of IoT since many of the devices that one would like to interconnect to the IoT (sensors, actuators, etc.) having limited power resources [21].

iv) Bluetooth 4.0 LE

Traditionally, Bluetooth is used in a connection-oriented manner and it cannot directly connect to the internet. Once it is connected; a link is maintained even there is no data flow. The new Bluetooth low energy (BLE), old name is WiBree, is a subset to Bluetooth v 4.0. It has new protocol stack and new profile architecture. This version has been adopted as of June 2010. It provides new adverting mechanism, quick discovery and enable connection and uses Asynchronous connection-less MAC for low latency rate and fast communication. Bluetooth 4.0 is users friendly as it introduces New Generic Attribute Profile which is simpler to use [22].

v) 6LoWPAN

The 6LoWPAN is Wireless PAN with low power and supports IPv6 network. It is a connection oriented technology in which router forward the data to its next hop to the 6LoWPAN gateway which is connected to 6LoWPAN with the IPv6 domain and then forward the data to its respected device correctly. With IPv6 we have enough address space to identify all the things in the world. In IP based network standard protocols (HTTP, TCP/IP) are directly applied on sensor nodes just as they do with traditional web servers out there in the Internet [23].

vi) Z-Wave

Z-Wave protocol architecture developed by ZenSys and promoted by the Z-Wave Alliance. It is another low power consuming which mostly used in automation and light commercial environment. It has an open communication protocol. The main purpose of Z-wave is for a reliable massage passing from a control unit to one or more nodes in the network. Z-wave have two types of devices, one is poll Controllers which send commands to the slaves, the second type of device, which reply to the controller to execute the commands [24] [25].

vii) Wi-Fi

Wireless fidelity is known as Wi-Fi, the IEEE 802.11x standards, is the most common way to connect devices wirelessly to the Internet. Laptop, Smartphone and Tablet PC are equipped with Wi-Fi interfaces and talk to wireless router and provide two way accesses to the Internet. The Wi-Fi standard family allows establishing wireless network on short distances. Wi-Fi has series types of networks like IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11e: QoS extension, IEEE 802.11f: extension for managing handover and IEEE 802.11i security extension. The Wi-Fi group is working on unlicensed spectrum of 2.4 GHz (ISM) band. The Table 1.1 summarizes all IoT communication protocol highlights:

Technology	Standard	Features	Application Areas
ZigBee	IEEE 802.15.4 standard	self-organizing, multi-hop, reliable mesh networking with long battery life	Home Automation, Smart Energy devices, lighting, HVAC.
RF Links	ISO & EPCglobal standard for RFID	low cost, high mobility and efficiency in identifying devices and objects	Smart cars keys, Smart Home keys, Smart Cards
Bluetooth	IEEE 802.15.1	short distance data sharing and devices mobility support	IoT monitoring and measuring applications
Bluetooth 4.0 LE	Subset to Bluetooth v 4.0	quick discovery, enable connection and uses, Asynchronous connection-less MAC for low latency rate and fast communication	connect PC peripherals into a powerful industrial and domestic IoT connectivity solution

6LoWPAN	Wireless PAN with low power supports IPv6	Small packet size, low power operated, Low bandwidth	asset tracking, environmental monitoring
Z-Wave	Z-Wave Alliance	reliable massage passing from a control unit to one or more nodes in the network	Used in automation and light commercial environment
Wi Fi	IEEE 802.11x	Low cost, Reliable, ease to deploy	smart home gadgets and appliances, digital signages or security cameras.

Table 1: IoT Communication Protocols Highlighted Features

2.7. 5G

IoT and 5G are new generation of technology. It represents a fundamental change in the mobile ecosystem, unleashing a powerful combination of extraordinary speed, expanded bandwidth, low latency, and increased power efficiency that is driving billions more connections in the next five years and changing our world. 5G is important to the Internet of Things because of the need for a faster network with higher capacity that can serve connectivity needs. The 5G spectrum expands the frequencies on which digital cellular technologies will transfer data. 5G has the potential to drive advancements in smart machines to smart manufacturing. 5G IoT reaches new dimensions in all aspects. The data throughput in the new network should reach up to 20 gigabits per second and allow shorter response times. With 5G, it will also be possible to transmit data in real time. This means that 100 billion mobile devices around the world would be accessible at the same time. That means a connection density of approximately one million devices per square kilometer. At the same time, the new technology brings an increase in the relative movement speed the connection quality will be much more stable up to a speed of 500 kilometers per hour, which will bring enormous benefits in future of IoT.

2.8. Semantic Search Engines

Semantic search technologies are those in which search engine searches the most accurate results in the large pool of data storage units independently by understanding [26]. It is predicted that successful applications of semantics on computers and will create new technologies that use human-readable and structured machine data to assist both humans and machines. It has already been introduced at the early stages of studying the IoT domain to deal with big data, interoperability and achieve actionable knowledge handling. Semantic Web technology permits IoT devices to "understand" and process data using structured and machine readable descriptions of resources [26]. Machine-interpretable data descriptions can also show where data originates from, how it can be related to its context, who provides the data, and what the various attributes of the data are. This framework guides how the semantically annotate and easily interpret information exchanged among IoT devices. In order to make and maintain effective business decisions, many organizations are leveraging external data sources from Semantic Web, e.g., social networks, media feeds, sensor data, or any other generic published information [27]. The integration of semantic principles and their application are supposed to improve the edition processes of IoT devices in the nearest future.

3. Enabling Technologies: Issues and Challenges

The involvement of IoT systems in all aspects of life made it complex and gave rise to several issues and challenges. These issues are also a challenge for the IoT developers in designing and adopting the advanced smart tech society. As technology is growing, challenges and need for advanced IoT system growing too. Hence, IoT developers need to take care of old issues; think about new issues arising and should provide solutions for them. Some of issues and challenges faced by involving enabling technologies of IoT are:

3.1 WSN

Wireless Sensor Networks is an important part of IoT applications. In an IoT environment Wireless sensor nodes are typically deployed for gathering sensitive information from unattended or hostile

environments and prominently exposed for security attacks; thus strongly affecting the user privacy and the network performance. Consequently, an exploration of the major and minor security requirements is necessary in the Wireless Sensor Networks for managing issues and challenges in WSN [28]. In order to allow WSN to become an intrinsic part of the IoT in a secure way, several security issues and challenges must be considered. These challenges are tightly related to WSN, but also can be applicable to other relevant technologies of the IoT [29]. These are:

a) **Devices Heterogeneity:** Connection of smart devices to other devices which are heterogenic in nature is major challenge while building IoT. Such devices run on different platforms, they use different protocols to communicate. So it is necessary to do unification of such devices.

b) **Scalability:** The scalability of the IoT plays a well-known challenge because every day new devices/objects are getting connected with the network. It involves issues like addressing/naming conventions, information management, service management etc.

c) **Ubiquitous data exchange through wireless technologies**: The wireless technologies are used to connect smart devices. It involves issues like availability, network delays, congestion etc.

d) **Energy-optimized solutions:** As many devices are connected via networks, energy spent for data communication will be high. The challenge is to optimize the use of energy required for communication between different devices.

e) **Localization and tracking capabilities:** The smart objects must be identified and tracking of them is required to maintain the security.

f) **Self-organization Capabilities:** It is required that the smart objects should sense the environment and autonomously react to real world situations, without much human intervention.

g) **Semantic interoperability and data management:** IoT exchange data among different smart objects, it is required that there should be a standardized format for data exchange in order to ensure the interoperability among applications.

h) **Embedded Security and privacy preserving mechanisms:** In IoT, security and privacy are the major issues in order to get acceptance from users. IoT technology should be secure and privacy-preserving by design. In spite of above issues some considerable challenges are:

i) **Ultra-large sensing device access:** The installation of WSN sensing devices in the future will grow exponentially due to the needs for comprehensive monitoring in transportation, electricity, industry and other critical infrastructures. An estimate by ABI Research, 50 billion new machine-to-machine (M2M) devices will appear in the next 10 years, and the number of the WSN devices will account for most of the scale [30]. As a result, how to cope with a very large scale of WSN device access is an important challenge.

ii) **Massive heterogeneous data processing:** With the large-scale application of WSN technology in the information and intelligence process of infrastructures, the amount of data produced by WSN sensors will grow from today's EB level (1 018 bytes) to ZB (1 021 bytes) level. According to IDC statistics and forecasts, in 2009, the global data volume was 0.8 ZB (1 021 bytes), and will be 35 ZB by 2020 [31]. As a major part of the data, the amount of sensing data from the physical world is 30 times more than that from human society. In this sense, the storage and transmission as well as timely treatment of mass data will be an unprecedented challenge. Intelligent control and services to dynamic changes

iii) **Intelligent control and services to dynamic changes:** Future operation and management of city infrastructures are required to meet the needs for safety, energy conservation, efficiency, convenience, etc. In the existing mode, information is automatically collected and processed through manual analysis, decisions and responses are made accordingly. Yet, this mode is no longer applicable. Intelligent control that is ready to respond to dynamic changes must be implemented. Firstly, WSN application mode should transform from simple perception to closed-loop control. For example, in intelligent transportation applications, to guarantee smooth urban transportation, it is necessary to make dynamic analysis on traffic conditions and real-time adjustments of traffic

lights. Nevertheless, the infrastructure control is of great significance, so ensuring the security and reliability of intelligent control will be a major challenge. Secondly, the WSN service mode should transform from the single and predefined into the dynamic and personalized. For example, in smart power utilization, to ensure both the user's electricity demand and improve the efficiency of grid operation, the setting of the air conditioning temperature and light levels should be dynamically adjustable in.

3.2 Cloud Computing

Since the IoT suffers from limited capabilities in terms of processing power and storage, it must also contend with issues such as performance, security, privacy, reliability. The integration of the IoT into the Cloud is certainly the best way to overcome most of these issues. The Cloud can even benefit from the IoT by expanding its limits with real world objects in a more dynamic and distributed way, and providing new services for billions of devices in different real life scenarios. There are many challenges which could potentially prevent the successful integration of the Cloud-based IoT paradigm. These challenges include:

a) Security and privacy

Cloud-based IoT makes it possible to transport data from the real world to the Cloud but an important issue which has not yet been resolved is how to provide appropriate authorization rules and policies while ensuring that only authorized users have access to the sensitive data; this is crucial when it comes to preserving users' privacy, and particularly when data integrity must be guaranteed [32]. Whenever serious IoT applications move into the Cloud, issues arise like lack of trust in the service provider, information regarding service level agreements (SLAs), and the physical location of data [33], [34]. Sensitive information breaching issues also does not solve by public key cryptography because of the processing power constraints imposed by IoT objects [32]. New challenges also require specific attention; for example, the distributed system is exposed to number of possible attacks, such as SQL injection, session riding, cross site scripting, and side-channel. Moreover, important vulnerabilities, including session hijacking and virtual machine escape are also problematic in the IoT trends [32], [35].

b) Heterogeneity

One particularly important challenge faced by the Cloud based IoT approach is related to the extensive heterogeneity of devices, platforms, operating systems, and services that exist and might be used for new or developed applications. Cloud platforms suffer from heterogeneity issues; for instance, Cloud services generally come with proprietary interfaces, thus allowing for resource integration based on specific providers [32]. In addition, the heterogeneity challenge can be exacerbated when end-users adopt multi-Cloud approaches, and thus services will depend on multiple providers to improve application performance and resilience [36].

c) Big Data

We know that cloud used to store big data generated by IoT devices; the related issues are storing this data during long period of time as well as need complex analysis for this [37]. Handling the huge amount of data produced is a significant issue, as the application's whole performance is heavily reliant on the properties of this data management service. Finding a perfect data management solution which will allow the Cloud to manage massive amounts of data is still a big issue [38]. Furthermore, data integrity is a vital element, not only because of its effect on the service's quality, but also because of security and privacy issues, the majority of which relate to outsourced data [32].

3.3 Big Data Analytics

IoT systems have the potential to solve many problems, but numerous challenges remain unaddressed. The solutions to some of these challenges are yet to be provided by big data and analytics solutions themselves, while others require concentrated efforts from the IoT community, hardware and platform vendors, governments, and policy makers. Exploiting the temporal

usefulness of IoT data have a profound impact on the digitized world. However, these data have a temporal aspect that can be useful in making real-time decisions, improving quality, and providing an excellent user experience. The following challenges faced by Big data analytics:

i) Exploiting the temporal usefulness of IoT: IoT data have a temporal aspect that can be useful in making real-time decisions, improving quality, and providing an excellent user experience. In typical IoT solutions, the insights from the IoT data are often either time consuming or not put into use immediately. This trend changes into a proactive one to make correlations, derive insights, and find seasonal, emerging, and diminishing patterns using IoT data [38]. In many critical industrial applications, these correlations, insights, and patterns can help increase operational efficiency and achieve effective control in real time. Therefore, we must implement solutions that can handle data at the device or gateway level where the IoT data from devices, sensors, and processes are initially received.

ii) Diversity Issue: The IoT paradigm has heterogeneous protocols, standards, and platforms. The industrial world also faces IT and OT integration issues that demonstrate much technological fragmentation. Although the IoT paradigm does not have a universal protocol, multiple protocols may co-exist because of the different requirements and their intended uses. Therefore, IoT systems may be unable to support multiple protocols in an extensible way. Intelligent gateway solutions [39-40], must provide seamless integration and interoperability between various protocols.

iii) Data management Issue: IoT data are valuable assets. With the exponential increase in the number of IoT devices, systems, and processes, new approaches, such as Data Lakes [41], have emerged to handle big data. Data Lakes stores structured and unstructured data without any pre-conceived notion of how these data will be used afterward. This approach does not have apply scheme mapping or query languages and can store any data without restrictions. However, Data Lakes introduces few issues such as insertion of any data and loss of agility. To avoid such issues, different techniques has been imposed [42].

iv) Security challenges: A major hindrance in the broad integration of IoT in industries lies in its security. Several challenges, such as the recent Dyn attack [43], underscore the importance of having secure IoT devices, platforms, and applications which otherwise can lead to major catastrophes, such as the successful execution of a massive DDOS attack. The IT professionals in these industries have their hands full with the security issues of BYOD [44,45] and the implementation of on-site cloud infrastructures in their organizations. Therefore, IoT security issues only add to their worries. Security is also not the first topic in the current IoT discussions and is still largely treated as a compulsory yet secondary subject. Such disregard can be attributed to the lack of organizational policies and the ambiguities in government laws [46]. To guarantee a successful implementation of IoT, solving these security issues must be given priority in the IoT realm.

3.4 Embedded systems

When it comes to developing embedded IoT devices, the hardware design is viewed as a critical component for the success of the IoT product. In order to ensure the embedded IoT product meets the required function, consumes low power, and is secure and reliable, a lot of challenges are faced by the embedded IoT device manufacturers during the hardware designing phase of these devices. Below are a few hardware design challenges of the embedded IoT devices [45].

i) Lack of Necessary Flexibility for Running Applications Over Embedded Systems: With the rising demand for connected devices, embedded systems need to work with heterogeneous devices and adapt to different networking architectures to cope-up with new functionalities and performances in the real-time environment. Due to this situation of increasing technology adoption and deployment of new applications, embedded system designers face several problems in terms of flexibility while developing embedded IoT systems such as:

- Problems in ensuring smooth integration of new services
- Difficulty in adapting to new environments

- Frequent changes in hardware and software facilities
- Issues in packaging and integration of small size chip with low weight and lesser power consumption
- Carrying out energy awareness operations, etc.

ii) The Security Crisis in Embedded System Design: All the IoT hardware products need to perform securely in the real-time embedded environment. Since all the embedded components operate in a highly resource-constrained and in physically insecure situations, engineers often face problems in ensuring the security of these embedded components. These systems have to be designed and implemented to be robust and reliable and have to be secure with cryptographic algorithms and security procedures. It involves different approaches to secure all the components of embedded systems from prototype to deployment.

iii) High Power Dissipation of Embedded System Design: Another increasingly aggravating limitation is power dissipation of microprocessor hardware design for getting the best performance out of real-time applications and devices. The persistent challenge is how to deploy an embedded system with an increasing number of transistors and with an acceptable power consumption ratio. There are two causes of high power dissipation in designing low-power embedded systems: First, because the power dissipation per transistor is increasing with the increase in gate density, the power density of system on chips is set to increase. Thus, the engineers must reduce overall embedded systems' power consumption by using efficient system architecture design rather than relying on process technology alone. Second, engineers focus on better performance with low power consumption by increasing the frequency of the system, which burns more power. Engineers need to pay more attention to design choices as well.

iv) Problems of Testing an Embedded System Design: For ensuring a reliable product design, conducting in-depth testing, verification, and validation is another challenge.

- Embedded Hardware Testing: This is similar to all the testing types where embedded developers use hardware based test tools. This refers to the embedded hardware tested for the system's performance, consistency, and validation as per the product requirement.
- Verification: Ensuring whether functional verification has been implemented correctly or not.
- Validation: Referring to ensure whether the product matches with the requirement and passes all the quality standards.

v) Inadequate Functional Safety of Safety-Critical Embedded Systems: Functional safety is considered a part of a product's overall safety. Embedded systems are considered as generalized control systems, which perform various control functions that require autonomy, reconfiguration, safety, fault-tolerance and need to eliminate all the unacceptable risks to meet functional safety requirements. These considerations highly influence their use in applications, where many functional loops are competing for the design of computational resources due to which, a number of timing and task-scheduling problems arise.

vi) Increased Cost and Time-to-Market: Apart from flexibility and security, embedded systems are tightly constrained by cost. In embedded hardware design, the need originates to derive better approaches from development to deployment cycle in order to handle the cost modeling or cost optimality with digital electronic components and production quantity. Hardware/software code-designers also need to solve the design time problem and bring embedded devices at the right time to the market.

3.5 Security Protocol and Architecture

IoT brought users huge benefits; however, some challenges come along with it. Cybersecurity and privacy risks are the primary concerns of the researchers and security specialists cited. These two are posing a considerable predicament for many business organizations as well as public organizations. Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This vulnerability is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet requiring novel security solutions [46].

i) **Security:** The IoT is diverse from traditional computers and computing devices, makes it more vulnerable to security challenges in different ways [47]: Many devices in the Internet of Things are designed for deployment on a massive scale. An excellent example of this is sensors. Usually, the deployment of IoT comprises of a set of alike or nearly identical appliances that bear similar characteristics. This similarity amplifies the magnitude of any vulnerability in the security that may significantly affect many of them. Similarly, many institutions have come up with guides for risk assessment conduction. This step means that the probable number of links interconnected between the IoT devices is unprecedented. It is also clear that many of these devices can establish connections and communicate with other devices automatically in an irregular way. These call for consideration of the accessible tools, techniques, and tactics which are related to the security of IoT. Even with the issue of security in the sector of information and technology not being new, IoT implementation has presented unique challenges that need to be addressed. The consumers are required to trust the Internet of Things devices and the services are very secure from weaknesses, particularly as this technology continues becoming more passive and incorporated in our everyday lives. With weakly protected IoT gadgets and services, this is one of the very significant avenues used for cyber-attacks as well as the exposure of the data of users by leaving data streams not protected adequately. The nature of the interconnection of the IoT devices means if a device is poorly secured and connected it has the potential of affecting the security and the resilience on the Internet internationally. This behaviour is simply brought about by the challenge of the vast employment of homogenous devices of IoT. Besides the capability of some devices to be able to mechanically bond with other devices, it means that the users and the developers of IoT all have an obligation of ensuring that they are not exposing the other users as well as the Internet itself to potential harm. A shared approach required in developing an effective and appropriate solution to the challenges is currently witnessed in the IoT [47].

3.6 Communication Protocol

New smart antennas (fractal antennas, adaptive antennas, receptive directional antennas, plasma antennas) that can be fixed in the objects and made of new materials are the communication means that will permit new advanced communications systems on chip. Modulation schemes, transmission rates, and transmission speed are also major issues to be undertaken. New advanced solutions need to be defined to efficiently support mobility of billions of smart things, possibly well-found with multiple heterogeneous network resources. Last but not least, network virtualization techniques are key to confirm an evolutionary path for the arrangement of IoT applications with secure Quality of Service (QoS) [48]. Wi-Fi IEEE 802.11x is wireless LAN. It provides point-to-point and point-to-multi point high speed and robust communication. It allows multiple users to connect in the same time period to same frequency band with minimum interference to the other users. Wi-Fi operates on three different non-interoperable technologies i) Frequency Hopping Spread Spectrum (FHSS) ii) Direct Sequence Spread Spectrum, iii) and Infrared (IR). Wi-Fi 802.11n Technology, based on Multiple Input Multiple Output (MIMO) technology is intended to increase the data rates upto 600 Mbps and onwards. IEEE 802.11i is known as (WPA–2) that enhances the cyber security and Advanced Encryption Standard (AES) which fulfill the IoT requirement. It is easy to install,

supports mobility of devices, and less expensive. The reliability and availability is achieved by applying proper path engineering and system design techniques. The proper implementation of massage acknowledgement, error correction algorithms, data buffering etc. enhances the reliability of massage transmission over wireless medium.

3.7 5G

The speed and bandwidth of 5G could effectively replace home internet connections currently using Wi-Fi. The Consumer Technology Association(CTA) has reported that 5G will reach speeds of 10 Gbps, making it 100 times faster than 4G. This means that while it would normally take six minutes to download a two-hour movie on 4G, that same download would take less than four seconds on 5G. Of course, making that kind of powerful technology a reality comes with some challenges along the way. Here are five that will likely play a prominent role in the dawn of 5G:

i) Frequency bands: Unlike 4G LTE that already operates on established frequency bands below 6GHz, 5G requires frequencies up to 300GHz. Some bands, better known as mm Waves, can carry far more capacity and deliver a 20-fold increase over LTE's fastest theoretical throughput. Wireless carriers still need to bid for the higher spectrum bands, as they build and roll out their respective 5G networks.

ii) Deployment and coverage: Though 5G offers a significant increase in speed and bandwidth, its more limited range will require further infrastructure. Higher frequencies enable highly directional radio waves, meaning they can be targeted or aimed — a practice called beamforming. The challenge is that 5G antennas, although able to handle more users and data, can only beam out over shorter distances. This means that antennas and base stations will likely be smaller in the 5G era, but more of them would have to be installed on buildings or homes to compensate for their shorter range. Cities will need to install extra repeaters to spread out the waves and extend range, while also maintaining consistent speeds in more densely populated areas. For this reason, it is likely that carriers will continue to use lower-frequency bands to cover wider areas until the 5G network matures.

iii) Costs to build and buy: Building a network is expensive – carriers will raise the money to do it by increasing customer revenue. Much like LTE plans incurred a higher initial cost, 5G will probably follow a similar path. And it's not just building a layer on top of an existing network, it's laying the groundwork for something new altogether. Total global spending on 5G is set to reach $88 billion (€78.4 billion) by 2023, according to Heavy Reading's Mobile Operator 5G Capex. Once it becomes truly viable, certain device segments will be connected in entirely new ways, particularly vehicles, appliances, robots and city infrastructure.

iv) Device support: There's plenty of buzz already generating around 5G-enabled smartphones and other devices. However, their availability will hinge on how expensive they are for manufacturers to make, as well as how quickly the network rolls out. Similarly, autonomous vehicle technology is already in the market in limited forms but fully autonomous vehicles are still years away. They are waiting on 5G deployment, as they would be driving blind without the super-fast network to communicate with. The concept behind the IoT is too predicated on a fast network that can tie devices and services together. That is one of the promises analysts have forecast for 5G's potential, but people will first want to see how much the additional speed will enrich their lives with related issues and challenges.

v) Security and privacy: Like any data-driven technology, 5G rollout will have to contend with both standard and sophisticated cybersecurity threats. Though 5G falls under the Authentication and Key Agreement (AKA), a system designed to establish trust between networks, it would currently be possible to track people nearby using their phones or even eavesdrop on live phone calls. With data speeds expected to be magnitudes faster than current levels, so too will connectivity increase. It will force cloud-based and data virtualization services to be as airtight as possible to

protect user data and privacy. In the same vein, their users will have to be more careful and vigilant, as stewards of their data. The rollout of a technology as life-changing as 5G won't be an easy one, and challenges are already starting to come to light as we step in to this new era of connectivity. Even so, the benefits far outweigh the issues, as the rollout of 5G also signals the dawn of autonomous vehicles, next-level smart cities and homes, and more. By building out infrastructure, updating policy, and rethinking the role we play in privacy, we all can do our part to prepare for the 5G era.

3.8 SEMANTICS IN THE IOT

Challenges of IoT are related to the possibility to consider relevant issues of the physical world, ensuring technical interoperability from technologies to deliver information, and ensuring a possibility for the information to be understood and processed. The challenges identified from related work which are related to semantic technologies in the IoT are organized in the following groups:

i) Scalability and flexibility: Properties of highly dynamic and distributed systems consisting of a large number of communicating objects indicate that scalability is to become one of major research problems and requires development of flexible and extendable solutions. The research in this area has to consider the following issues: automated (or semi-automated) annotation of available resources, semantic association discovery and analysis (resource connection or activation), and efficient solutions to create, analyze and explore linked IoT data of various resources [49]. Some studies in the IoT domain address the rising problem of ensuring IoT scalability [50]. While using known P2P (peer-to-peer) methods for IoT systems promises good scalability possibilities.

ii) Standardization and Reusability: Standardization is a vital area of concern in any data engineering field as it infers stable quality levels over time and steadiness against unexpected faults. Technical standards are based on consensus of different parties involved in development or production of a given service or device. It is essential to define and follow a standard specification guide so that further enhancements can be added to existing solutions without significant effort [51]. The idea of standardization of IoT interconnected devices on a global scale is improbable at this point; however, certain regulatory approaches are aiming at standardization [52]. The European Commission provides open framework guidelines for development of IoT devices for ensuring that such principles as verticality, ubiquity, and technicity are well aligned. However, they only apply to Europe and by no means can be considered a global measure.

iii) High level processing: Large scale of resource heterogeneity and distribution in IoT entails a need for notable computational power. Full potential of IoT will be leveraged by transforming low-level data into high-level data seamlessly and in a comprehensive way [49]. Low-level data are single observation and measurement units captured by sensors or other devices. Usually IoT data consumers, either humans or machines, are not interested in unit measurements but rather in high level contextual meaning of data. Such high-level abstractions should be machine interpretable for computers and human-understandable for humans. High-level knowledge collection, transfer, data extraction and modification in a specific domain for certain applications are demanding the largest part of processing resources. Currently there are only some solutions that address this problem. For instance, the annotation tool in Sense2Web creates an opportunity for users to annotate sensor data such as resource, entity, and service descriptions.

iv) Data quality: Semantic Web development has produced a high volume of data being published on the web as Linked Open Data [23]. Some semantic description models such as the W3C SSN ontology offer attributes to describe qualitative aspects of data [49]. Analysis of such data quality reveals that these data often are not consistent. As stated, data extracted from partly structured or non-structured sources such as DBpedia might contain inaccuracies and misrepresentations. For human interpretation, inaccurate data might be sufficient. For machine-learning or knowledge-

dependent application, however, such data might be unacceptable. While many methodologies and frameworks exist for assessing data quality and deriving appropriate conclusions and suggestions for improvement, the Web of Data contains innovative aspects that are not always covered by existing mechanisms. As data volume increases, inconsistency and redundancy become troubling issues. Inconsistent data detection for distributed networks becomes even more challenging.

v) Data confidentiality and privacy: By means of big data analytics and web mining techniques, behavior of user can be analyzed to improve structure and content of offered services. The helping a user to feel more comfortable and enabling intuitive browsing uncover methods and approaches of utilizing user data for malicious means, thus threatening user privacy and confidentiality. Determining threatening behavior contexts is a ceaseless challenge. Large networks consisting of autonomous heterogeneous devices as in IoT transfer large amounts of valuable information. These kinds of systems will not only own and record information about users but will also produce sensitive data that are rich in context [53].

4. Future Research Directions

The IoT can best be described as a CAS (Complex Adaptive System) that will continue to evolve hence requiring new and innovative forms of software engineering, systems engineering, project management, as well as numerous other disciplines to develop it further and manage it the coming years. This has become even more evident, as different governments around the world have shown an interest in the IoT concept by providing more funding in the field that is meant to facilitate further research. As more and more research studies are conducted, new dimensions to the IoT processes, technologies involved and the objects that can be connected, continue to emerge, further finding way for much more application functionalities of IoT. The fact that IoT is so expansive and affects practically all areas of our lives, makes it a significant research topic for studies in various related fields such as information technology and computer science, economic development, water quality maintenance, well-being, industrialization etc. IoT is transforming the traditional civil structure of the society into high tech structure with the concept of smart city, smart home and smart vehicles and transport. Rapid improvements are being done with the help of supporting technologies such as machine learning, natural language processing to understand the need and use of technology at home. Various technologies such as cloud server technology, wireless sensor networks that must be used with IoT servers to provide an efficient smart city. Another important issue is to think about environmental aspect of smart city. Therefore, energy efficient technologies and Green technologies should also be considered for the design and planning of smart city infrastructure. While need to combine agriculture with technology so that the production can be improved in an efficient and new research way. Greenhouse technology is one of the possible approaches in this direction. It provides a way to control the environmental parameters in order to improve the production. Thus New technologies must necessarily be coupled to existing models and should serve as axes for the creation of new models.

5. Conclusion

Recent advancements in IoT have drawn attention of researchers and developers worldwide. IoT developers and researchers are working together to extend the technology on large scale and to benefit the society to the highest possible level. However, improvements are possible only if we consider the various issues and shortcomings in the present technical approaches listed in chapter. In this chapter, we presented several issues and challenges that IoT developer must take into account to develop an improved model. Also, important application areas of IoT is also discussed where IoT developers and researchers are engaged. As IoT is not only providing services but also has without a doubt a massive capability to be a tremendously transformative force, which will, and to

some extent does already, positively impact millions of lives worldwide so need to be pay attention at each and every aspect of IoT.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.
[2] Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. In: Proc. 2017 international conference on smart, monitored and controlled cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017.
[3] Gatsis K, Pappas GJ. Wireless control for the IoT: power spectrum and security challenges. In: Proc. 2017 IEEE/ACM second international conference on internet-of-things design and implementation (IoTDI), Pittsburg, PA, USA, 18–21 April 2017. INSPEC Accession Number: 16964293. K. Ashton, ‘‘Internet of Things,’’ RFID J., vol. 22, no. 7, pp. 97–114,
[4] K. Ashton, ‘‘Internet of Things,’’ RFID J., vol. 22, no. 7, pp. 97–114, 2009.
[5] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, ‘‘Internet-ofThings-based smart environments: State of the art, taxonomy, and open research challenges,’’ IEEE Wireless Commun., vol. 23, no. 5, pp. 10–16, Oct. 2016.
[6] L. Atzori, A. Iera, and G. Morabito, ‘‘The Internet of Things: A survey,’’ Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[7] Gupta N, Gupta J. Internet of Things (IoT): a vision of any-time any-place for any-one. Int Rob Auto J. 2017;2(6):234–240. DOI: 10.15406/iratj.2017.02.00041
[8] Karen Rose, Scott Eldridge, Lyman Chapin, “The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World”, The Internet Society (ISOC), 2015.
[9] Alem Čolaković, Mesud HadžialiInternet of Things (IoT): A review of enabling technologies, challenges, and open research issues”, ttps://doi.org/10.1016/j.comnet.2018.07.017
[10] R. Minerva, A. Biru, and D. Rotondi. (May 27, 2015). Towards a Definition of the Internet of Things (IoT) Accessed: Jan. 03, 2019. [Online]. Available: http://iot.ieee.org/images/files/pdf/IEEE_ IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
[11] R. Buyya, C. Shin, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: Vision , hype , and reality for delivering computing as the 5th utility,” Futur. ener. Comput. Syst., 2009, pp. 599–616.
[12] Ejaz Ahmeda,∗ , Ibrar Yaqooba , Ibrahim Abaker Targio Hashema , Imran Khanb , Abdelmuttlib Ibrahim Abdalla Ahmeda , Muhammad Imranc , Athanasios V. Vasilakos d, http://dx.doi.org/10.1016/j.comnet.2017.06.013 1389-1286/© 2017 Elsevier
[13] J.L. Pérez, D. Carrera, Performance characterization of the serviotic api: an iot-as-a-service data management platform, in: Big Data Computing Service and Applications (BigDataService), 2015 IEEE First International Conference on, IEEE, 2015, pp. 62–71
[14] Rydhm Beri, “Embedded System in IoT” IJIRCS July 2018, Available at http//www.davasrijircs.in International Journal of Innovation & Research in Computer Science Issue 5th ISSN:2349-2783
[15] Pal, S.; Hitchens, M.; Varadharajan, V. Modeling Identity for the Internet of Things: Survey, Classification and Trends. In Proceedings of the 2018 12th International Conference on Sensing Technology (ICST), Limerick, Ireland, 3-6 December 2018; pp. 45–51.
[16] Aqeel-ur-Rehman, K. Mehmood, and A. Baksh,” Communication Technology that suits IoT: A critical Review “, Conference Paper · April 2013 DOI: 10.1007/978-3-642-41054-3_2
[17] Hosenkhan, M.R.; Pattanayak, B.K. Security Issues in Internet of Things (IoT): A Comprehensive Review. In New Paradigm in Decision Science and Management; Springer: Berlin/Heidelberg, Germany, 2020; pp. 359–369.
[18] Alam, S.; Siddiqui, S.T.; Ahmad, A.; Ahmad, R.; Shuaib, M. Internet of Things (IoT) Enabling Technologies, Requirements, and Security Challenges. In Advances in Data and Information Sciences; Springer: Berlin/Heidelberg, Germany, 2020; pp. 119–126.
[19] Li, Y.; Gao, M.; Yang, L.; Zhang, C.; Zhang, B.; Zhao, X. Design of and research on industrial measuring devices based on Internet of Things technology. Ad. Hoc. Netw. 2020, 102, 102072. [CrossRef]
[20] International Telecommunication Union UIT. ITU Internet Reports 2005: The Internet of Things[R] (2005)
[21] ZigBee – The Internet of Things, http://www.vesternet.com/zigbee (accessed on November 2012)

[22] Decuir, J.: Bluetooth 4.0: Low Energy, IEEE Annual Report (2010), http:// chapters.comsoc.org/vancouver/BTLER3.pdf (accessed on October 2012)
[23] Ee, G. K., Ng, C. K., Noordin, N. K., Ali, B. M.: A Review of 6LoWPAN Routing Protocols. In: Proceeding of Asia Pacific Advanced Network (2010)
[24] Sarma, A.C., Girão, J.: Identities in the future internet of things. Wireless Personal Communications 49(3), 353–363 (2009)
[25] http://www.savingtrust.dk/publications/concepts/destsconcept-for-energy-saving-devices-metering-equipment-andwireless-communication (accessed on December 2012)
[26] D. Pfisterer, D. Pfisterer, K. Romer, D. Bimschas, O. Kleine, R. Mietz, C. Truong, H. Hasemann, A. Kröller, M. Pagel, M. Hauswirth, M. Karnstedt, M. Leggieri, A. Passant, R. Richardson, "SPITFIRE: Toward a Semantic World"
[27] D. Boyd and K. Crawford, "Six Provocations for Big Data," Computer and Information Science, vol. 123, 2011.
[28] *M. A. Burhanuddin, Ali Abdul-Jabbar Mohammed, Ronizam Ismail, Mustafa Emad Hameed, Ali Noori Kareem, Halizah Basiro* ,"A review on security challenges and features in WSN: IoT prespective", Vol 10, No 1-7, *ISSN: 2180-1843*
[29] Ashvini Balte*, Asmita Kashid, Balaji Pati, " Security Issues in Internet of Things (IoT): A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, 2015.
[30] DUNLAP, J. From billing & technology convergence to ecosystem convergence: Why M2M matters to your business. Pipeline: Technology for Service Providers, Vol. 8, No. 7, 2011, pp. 13.
[31] FELDMAN, S. Unif ed information access: Creating information synergy. IDC, 2012.
[32] G. Suciu A. Vulpe S. Halunga O. Fratu G. Todoran V. Suciu "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things" 19th Int. Conf. Control Systems and Computer Science (CSCS) 2013, pp. 513-518.
[33] A. Alenezi, N. H. N. Zulkipli, H. F. Atlam, R. J. Walters, and G. B. Wills, "The Impact of Cloud Forensic Readiness on Security," in 7st International Conference on Cloud Computing and Services Science, 2017, pp. 1–8.
[34] K. S. Dar, A. Taherkordi and F. Eliassen, "Enhancing Dependability of Cloud-Based IoT Services through Virtualization," 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), 2016, pp. 106-116
[35] C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," Proc. - 6th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS, 2012, pp. 922–926
[36] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, "An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things," in 2nd International Conference on Internet of Things, Big Data and Security, 2017, pp. 1–8
[37] A. Botta, W. de Donato, V. Persico and A. Pescapé, "On the Integration of Cloud Computing and Internet of Things," 2014 International Conference on Future Internet of Things and Cloud, Barcelona, 2014, pp. 23-30
[38] S. Aljawarneh, V. Radhakrishna, P. V. Kumar and V. Janaki, "A similarity measure for temporal pattern discovery in time series data generated by IoT," *2016 International Conference on Engineering & MIS (ICEMIS)*, Agadir, Morocco, 2016, pp. 1-4, doi: 10.1109/ICEMIS.2016.7745355.
[39] P. Desai, A. Sheth and P. Anantharam, "Semantic Gateway as a Service Architecture for IoT Interoperability," 2015 IEEE International Conference on Mobile Services, New York, NY, USA, 2015, pp. 313-319, doi: 10.1109/MobServ.2015.51.
[40] A. Meddeb, "Internet of things standards: who stands out from the crowd?," in IEEE Communications Magazine, vol. 54, no. 7, pp. 40-47, July 2016, doi: 10.1109/MCOM.2016.7514162.
[41] H. Fang, "Managing data lakes in big data era: What's a data lake and why has it became popular in data management ecosystem," 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Shenyang, China, 2015, pp. 820-824, doi: 10.1109/CYBER.2015.7288049.
[42] Rihan et al., "Constance: an intelligent Lake system", SIGMOD/PODS'16: International Conference on Management of Data San Francisco California USA June, 2016
[43] C.chris.mishler"The future of Internet things : strategic finance" htttp://refhub.elsevier.com/S1389-1286(17)30259-1/sbref0065

[44] S. Tanimoto, S. Yamada, M. Iwashita, T. Kobayashi, H. Sato and A. Kanai, "Risk assessment of BYOD: Bring your own device," *2016 IEEE 5th Global Conference on Consumer Electronics*, Kyoto, Japan, 2016, pp. 1-4, doi: 10.1109/GCCE.2016.7800494.
[45] https://dzone.com/articles/top-6-hardware-design-challenges-of-the-embedded
[46] Tawalbeh, L.A.; Tawalbeh, H. Lightweight crypto and security. In Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications; Wiley: West Sussex, UK, 2017; pp. 243–261.
[47] Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. J. Netw. Comput. Appl. 2017, 88, 10–28. [CrossRef]
[48] Aqeel-ur-Rehman , Kashif Mehmood, and Ahmed Baksh," Communication Technology That Suits IoT – A Critical Review", WSN4DC 2013, CCIS 366, pp. 14–25, 2013. © Springer-Verlag Berlin Heidelberg 2013
[49] P. Barnaghi, W. Wang, C. Henson and K. Taylor, "Semantics for the Internet of Things," Int. J. Semant. Web Inf. Syst. vol. 8, no. 1, pp. 1–21 2012.
[50] Gyrard, S.K. Datta, C. Bonnet and K. Boudaoud, Standardizing Generic Cross-Domain Applications in Internet of Things. 2014 IEEE Globecom Work. GC Workshops 2014, pp. 589–594, IEEE, 2014
[51] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context Aware Computing for the Internet of Things: A Survey," IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 414–454, 2014.
[52] R.H. Weber, "Internet of Things – New Security and Privacy Challenges," Comput. Law Secur. Rev. vol. 26, no. 1, pp. 23–30, 2010.
[53] C.-W. Tsai, C.-F. Lai and A.V. Vasilakos, "Future Internet of Things: Open Issues and Challenges," Wirel. Networks, vol. 20, no. 8, pp. 2201– 2217, 2014. https://doi.org/10.1007/s11276-014-0731-0