JACET

J. ADV COMP ENG TECHNOL, 4(2) Spring 2018

Statistical Analysis on IoT Research Trends: A Survey

Mehrin Rouhifar[1], Sahar Bahramzadeh[2], Alireza Hedayati[3], Vahe Aghazarian[4] and Mostafa Chahardoli[5]

1,2,3,4,5 Department of Computer Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran.

3 (hedayati@iauctb.ac.ir)

Received (2018-04-23) Accepted (2018-06-21)

Abstract: *Internet of Things (IoT) is a novel and emerging paradigm to connect real/physical and virtual/logical world together. So, it will be necessary to apply other related scientific concepts in order to achieve this goal. The main focus of this paper is to identify the research topics in IoT. For this purpose, a comprehensive study has been conducted on the vast range of research articles. IoT concepts and issues are classified into some research domains and sub-domains based on the analysis of reviewed papers that have been published in 2015 & 2016. Then, these domains and sub-domains have been discussed as well as it is reported their statistical results. The obtained results of analysis show the most of the IoT research works are concentrated on technology and software services domains similarly at first rank, communication at second rank and trust management at third rank with 19%, 14% and 13% respectively. Also, a more accurate analysis indicates the most important and challenging sub-domains of mentioned domains which are: WSN, cloud computing, smart applications, M2M communication and security. Accordingly, this study will offer a useful and applicable broad viewpoint for researchers. In fact, our study indicates the current trends of IoT area.*

Keywords: *Internet of Things, Trends, Statistical analysis, Classification, Research domains and sub-domains.*

How to cite this article:

Rouhifar M, Bahramzadeh S, Hedayati A, Aghazarian V, Chahardoli M. Statistical Analysis on IoT Research Trends: A Survey. J. ADV COMP ENG TECHNOL, 4(2) Spring 2018 : 101-134

I. INTRODUCTION

AS the mobile computing and wireless communications develop, a new paradigm called Internet of Things (IoT) has been created and has attracted the attention of many researchers in industry and research area. IoT can be described as a pervasive network the aim of which is to provide a system to monitor and control physical world by collecting, processing, and analyzing of data which sensor devices in IoT generate. These devices are used for sense and communication interfaces, and they contain of sensors, radio frequency identification devices (RFID), global positioning system devices (GPS), actuators, Local Area Network (LAN) interfaces and etc [1]. There are plenty of survey articles about Internet of Things, which each of them has studied IoT in a specific field or a limited range of concepts and related challenges (based on conducted investigations). Whereas, for the first time in this paper, it has been attempted to study and discuss all concepts of IoT with a macro viewpoint in domains and sub-domains structure, and review issues and related challenges in order to determine the current research trends. Therefore, some fundamental concepts and several important articles in various areas are referred in the following.

One of the most important issues in IoT area is communications. Since "things" can connect to internet, and therefore, can be remotely controlled, hence, Machine to Machine (M2M) communications have been created from the communication's main paradigm of the emerging IoT. This makes the integrated exchange of information, among the independent devices, possible without any human interactions [2]. According to the definition that International Telecommunication Union (ITU) and IoT European Research Cluster (IERC) present, IoT, as the global network infrastructure, is capable of self-configuration, which is based on the standard and compatible communication protocols. Physical and virtual things have identities, and are connected together through intelligent interfaces [1]. For this purpose, routing protocols are required that be able to connect things in a non-centralized, self-organized and variable infrastructure. Therefore, communication protocols and technologies play an important key role in IoT [3]. In [4], has been discussed the IoT protocol stack, which presented by Internet Engineering Task Force (IETF). Also in order to support ever increasing number of emerging applications, Media Access Control (MAC) sub-layer of the wireless networks and routing protocols have to be inherently scalable and interoperable [5].

Another issue is architecture standardization. It can be considered as the IoT backbone, which creates a competitive environment for companies and manufacturers to supply productions with high quality. Also, traditional internet architecture should be modified for adapting to the IoT challenges [6]. Different types of architecture have been proposed for IoT by standardization institutes and industry. All these architectures have layered structures, and regarding functionality, they are common at two layers of device and network. But so far, IoT has been without a unique architecture. Layered architecture in industrial IoT has been discussed in [7]. Presenting a proper layered architecture is one of solutions to increase scalability.

As it was mentioned before, mostly things like sensors and mobile devices with internal connections sense and monitor the environment and collect different types of data. Collected information for an application highly tends to be correlated [8], so they can be aggregated or processed jointly while they are transmitted to sink. For example, fusion aggregates different sensors data, which are related to a physical event. Such data aggregation processes reduce the total number of transmitted messages on the wireless links, which can have a significant effect on energy consumption, as well as on the whole network performance. Therefore, a very important problem in data aggregation is to determine an optimal flow of information, and a communication topology in order to efficient routing of correlated data into the processing nodes [9].

Most of the nodes in IoT are battery-operated, and this issue makes the energy efficiency for appropriate performance and sensors management to be critical. Energy efficiency and its enough amount existence in IoT sensor nodes lead to creating research fields. IoT nodes have limited energy, and also because of interconnecting to different nodes, they consume energy. Therefore, many low-powered communication technologies have been developed, which are considered as enabling technologies [1]. On the other hand, each of physical things in IoT identified by a unique identifier and connects to internet without any need for human interactions. Long term and self-stable operations are key elements to realize such complicated networks, and require energy-aware devices, that are potentially able to harvest their required energy from environmental resources. Mentioned procedure is known as the energy harvesting method [10]. Therefore, considering the resource constraint of devices as well as the dynamic and heterogeneous nature of resources in IoT, energy management and consequently resource management will be necessary.

IoT devices generate huge volume of data. Since the generation and transmission of some IoT data is related to personal devices, so the need for security and privacy preservation is necessary. Therefore, trust management in IoT plays an essential and fundamental role in data mining, reliable data fusion, context-aware services, user privacy-preserving, and information security. Trust is a complex concept considering issues such as confidence, belief, reliability, integrity, security, and other features of an entity [11].

The other challenge is about software services.

Since in recent years, the development of IoT and connected physical devices and their virtual display have been a growing trend, so, supports a comprehensive show of physical environment and good level of interaction with actual world. A wide range of various new potential services and productions have been created in different areas such as logistics, smart homes, e-health, automation, Intelligent Transportation System (ITS), business/process management, and environmental monitoring [12]-[14]. In addition, the existence of a middleware is necessary in order to make the development of applications and other services easier in IoT [15].

The rest of this paper is organized as follows: Section 2 explains the classification approach of conducted studies about IoT and each of the domains and its sub-domains have been discussed in subsections respectively. Section 3 shows obtained statistic results of the exact analysis of conducted studies in different fields of IoT in the recent two years. Finally, in section 4 is presented the conclusion of paper.

II. CLASSIFICATION APPROACH

The aim of this study is to investigate current trends of IoT researches. To do so, a comprehensive study and review has been conducted on the vast range of valuable research references, which have the significant portion in the advancement of the science and technology including IoT. For this purpose, 339 papers have been investigated. These articles have been identified by searching the terms "Internet of Things" and "IoT" in database of various journals from famous and valid scientific publications such as Elsevier, IEEE, Springer, and ACM that have been published in 2015 & 2016. Table I. shows the exact number of articles related to each of the above publications in terms of year separately. As it is seen, a high percentage of studied papers belong to IEEE Xplore and then Elsevier.

TABLE I. Number of papers based on publications and year

	2015	2016
IEEE	136	41
Elsevier	30	77
Springer	38	13
ACM	0	4

In this paper, Internet of Things basic concepts have been classified into research domains and sub-domains using a top-down approach. For this purpose, a comprehensive study has been conducted in IoT area and its concepts are categorized into maximum three levels of keywords: Major Keywords, Level 1 Minor Keywords, and Level 2 Minor Keywords. Then, title of the articles has been analyzed one by one and their keywords have been extracted. Therefore, each paper can be considered in one domain and or more than one. In this regards, if the title of the article is not clear enough, will be necessary to study the abstract and sometimes conclusion section. All 339 articles were analyzed and classified into some domains and sub-domains. Afterward, according to the number of each of keywords, the IoT research trends have been determined, so that statistical results related to each of topics will be presented below in section 3.

Major Keywords are considered as domains. Accordingly, all top level concepts of IoT area have been classified into 9 main research domains which are: architecture, communication, trust management, technology, resource management, energy management, software services, data stream, and infrastructure/hardware, all illustrated in Fig. 1.

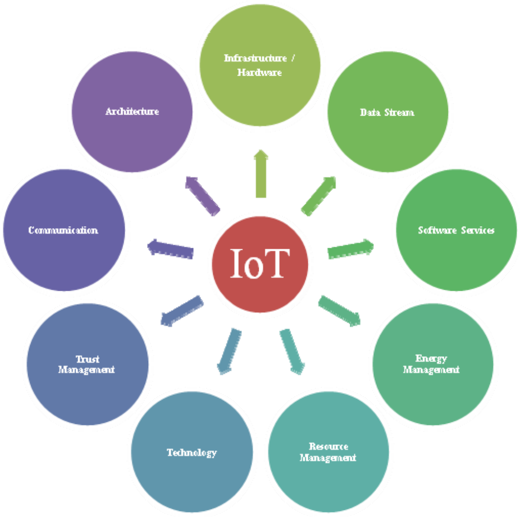

Fig. 1. IoT Research Domains Classification

Then, main domains are classified into some sub-domains according to their content as Level 1 Minor Keywords. Finally, some of these sub-domains are categorized into other sub-domains again (which are sub-subdomains) and in fact, they are Level 2 Minor Keywords. Fig. 2 indicates the summary of our proposed classification scheme up to 2 levels. In the following, mentioned domains and sub-domains are discussed in detail.

1. Architecture

One of the basic needs in IoT is that all things have to be connected together. IoT system architecture should support IoT operations which create a bridge between the physical and virtual world. Designing IoT architecture has many factors such as network, communications, processes, commercial models, and security. In this regards, different architecture models for IoT have purposed in recent years which have been discussed in this section and also, since the aim of majority of reviewed middleware articles was to present new layering of middle-layer in architecture and new integrator layer for heterogeneous processes in the architecture, so the papers of middleware concept is also discussed in this section. Therefore, this section of paper contains two subsections: architecture models, and middleware design methods.

1.1. Architecture Models

In designing IoT architecture, extensibility, scalability, and interoperability among the heterogeneous devices and their commercial models should be considered. Since there is the possibility of things mobility, and consequently there is need for real-time interactions, IoT architecture should be adaptive in order to let devices interact and connect with other things without ambiguity. Moreover, IoT should have heterogeneous and decentralized nature. There are several ideas proposed to design layered architecture in IoT, some of which are three layers [16-18], four layers (IoT-A project), or five layers [6]. Some cases of existing architectures have been mentioned in the followings.

International Telecommunication Union (ITU) has suggested a design in which IoT architecture is composed of four layers named Device, Network, Service Support & Application Support (middleware), and Application Layers. This type of architecture has also security and management capabilities, which are associated with all four mentioned layers (ITU-T Y.2060 Project).

Architectural Reference Model (ARM) architecture is the output of the IoT-A project, and is a reference architecture for Internet of Things [19] which has been designed based on the needs of researchers and industry [6]. Since, in the present world, each of smart networks has been designed and implemented based on its own specific architecture, and is inconsistent with others, therefore, a comprehensive architecture is required for IoT implementation so that different networks can operate based on an uniform infrastructure while they are maintaining interoperability, support and interconnection. In the ARM architecture, IoT functional model consists of nine functionality groups (FG), with seven longitudinal FGs, and two transversal FGs [20]. This architecture has hierarchical model.

In the following, another type of architecture, named Service-Oriented Architecture (SOA) is described [21]. In SOA, services are always executed by things located in a heterogeneous network. SOA architecture contains of four layers as: Sensing Layer, by which smart systems or sensors

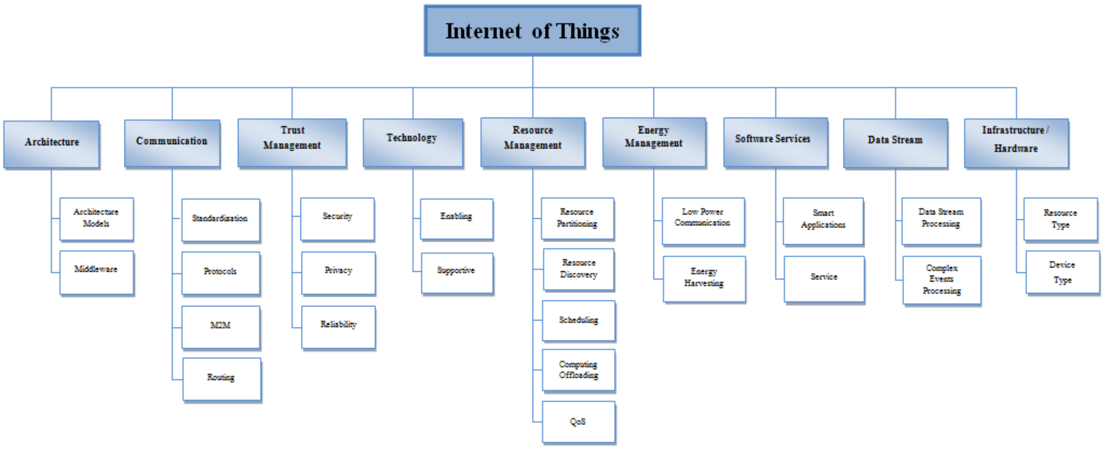

Fig. 2. IoT Research Sub-domains Classification

are able to sensing and data exchange among the different devices; Network Layer which not only connect things together, but also makes it possible to share information; Service Layer, which is based on middleware technology and does the key and fundamental operations in order to provide integrated services and applications in IoT; Interface Layer, which is used to create interoperability among heterogeneous things in order to data exchanging, communicating and events processing.

Based on the Gartner's definition, Web Oriented Architecture (WOA) is an improved version of SOA architecture which aggregates users and systems by using a web of globally linked hypermedia, based on the web architecture. This type of architecture is focused on the generality of interfaces (user interfaces and APIs). Thus, WOA can be considered as a combination of SOA, WWW, and REST features (WOA).

At the end of this subsection, API (Application Programming Interface) based architecture is discussed. In methods based on web APIs and REST, all required resources change from network bandwidth to the computing capability and storage capacity, and data conversion which is based on request/response method is triggered regularly during service call [22]. To do so, it is suggested SIMORGH in [23] that devices, sensors, human, and existing services are described by using web API symbol and API description languages. Similarly in [24] a service layer of broker named FOKUS has been presented which shows a collection of APIs to activate a shared access to OpenMTC core.

1.2. Middleware

Since IoT is a network consists of heterogeneous devices in infrastructure level, middleware can make the process of developing applications easier by integrating heterogeneous processes and communications. In fact, a middleware is a layer that is located between application layer and infrastructure, and supports management of services, resources, data, events, security, stability and many other type requirements [15].

Middleware is divided into several categories based on the different design approaches in accordance with [15]:

- event-based
- service-oriented
- VM-based
- agent-based
- tuple-spaces
- database-oriented
- application-specific

In some works, design approach of proposed middleware is hybrid. That means it has been designed in the form of combination of two above approaches. Below, there are some examples of similar works which have been done in recent two years.

Recently proposed middleware is designed for intelligent logistics field [25]. One of the challenges in logistics discussion is the integration of small services, and the integration of various heterogeneous IoT devices, in order to build high level services to make smart the commercial logistics processes. In this type of middleware that has the advantages of SOA architecture, distribution of information related to service composition and finding proper composed services for tasks of each commercial process are done by a series of agents (task agent and resource agent). Therefore, this middleware approach can be seen as a combination of two types of service-oriented and agent-based middleware.

One of the other works is a presented middleware in [26] which is an event-based middleware (or Publish/Subscribe). This type has been applied for mobile crowed sensing systems. This middleware consists of two important software components, named cloud broker and mobile broker. Publishers are sensors which collect environmental data, and these data are transmitted through mobile broker (and directly sometimes) to the cloud broker, where required processing is done and then obtained results are notified in message format to mobile devices processes, which have subscribers role. Classification of middleware papers and architecture models papers are shown in Table II.

2. Communication

Concepts and challenges related to the communication scope have wide range. According to the most of important studied papers in this field, some of topics such as standardization, protocols, M2M communications and routing are very challenging and have been attracted the attention of a large number of researchers in comparison with others. IoT network composed of numerous heterogeneous things to connect with each other by using the communication protocols and technologies based on legalized standards. Although our classification mentions that routing concept is a subsection of protocols, but due to its importance as a main topic is written separately from it. Therefore, this domain is classified in the way that be involved all of the mentioned cases. The continuation of discussion describes them with more details.

2.1. Standardization

Standardization and limitations of monitoring policies have challenged cases like development rate in Internet of Things. This reality can potentially barricade to be accepted technologies. So, defining and propagating standards make it easier to apply and use IoT environments for new users and providers. In other words, if pervasive and global standards for IoT are introduced and applied [28], it will greatly

TABLE II. Classification of Architecture Domain Papers

IoT Domain	Sub-domain	Research Field	References (Papers)
Architecture	Architecture Models	ARM (IoT-A)	[6] [20]
		SOA	[21]
		API – Based	[22]
	Middleware	Event-based	[26]
		SOA-based	[27]
		Agent-based & SOA-based	[25]

affect interoperability among the different components, services providers, and even end users [29]. IoT standards and related protocols are proposed by different groups such as World Wide Web Consortium (W3C), IETF, EPCglobal, Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI) [6]. Regulations about accessibility of radio frequency levels, creating enough level of interoperability among different devices, authentication, identification, permission and communication protocols, are open challenges related to IoT standardization [21]. In this paper, all required communication standards for development of IoT are considered in this category.

2.2. Communication Protocols

From the viewpoint of network and communications, IoT can be considered as a set of different networks including mobile networks (3G, 4G, CDMA and etc), Wide Networks (WLANs), Wireless Sensors Networks (WSN), and Mobile Ad-hoc Networks (MANET) [30].

Integrated connections are basic and main requirements for IoT that communication technologies satisfy such necessities properly. According to [6], many communication protocols are well known such as WiFi [31], Bluetooth [32], IEEE 802.15.4, Z-Wave, Zigbee [33], Advanced LTE (Advanced Long-Term Evolution). Also, there are several new emerging options like Thread, Neul, LoRa and Sigfox. Meanwhile, some specific types of communication technologies in IoT are Radio Frequency Identification (RFID) [34], Near Field Communication (NFC) [35] and Ultra-Wide Bandwidth (UWB).

As mentioned above, communication protocols are required to interconnect the things in IoT environments. In [22], protocols in Internet of Things have been classified into three categories: 1) General-purpose protocols like IP (Internet Protocol) [36], [37] and SNMP (Simple Network Management Protocol), which are used for management, monitoring, configuration of network devices and creating communication links in wide area; 2) Lightweight protocols, like CoAP (Constrained Application Protocol), which are developed to satisfy the needs of devices with small hardware and constrained resources [37], [38]; and 3) Specific protocols of device or vendor, and APIs that usually need specific set of tools. More details about the communication protocols of different layers are accessible in [39].

2.3. M2M Communication

Mobile communication of machine to machine (M2M) is one of the emerging areas of common communication among the various smart systems [40]. M2M implicates independent communication among same type devices with specific applications which are connected to each other through wireless or wired communication networks. M2M communication has especially developed to achieve profitable efficiency, low cost, and high security and safety [19]. Communication protocols in IoT use two models of messages exchanging, named Publish/Subscribe, and Request/Response. Publish/subscribe model is a common method of messages exchanging in distributed environments and dynamic scenarios. It is accepted by popular M2M communication protocols like MQTT (Message Queue Telemetry Transport). Protocols such as HTTP/REST (Hypertext Transfer Protocol/Representational State Transfer) and CoAP support only Request/Response model [29], [41]. Many M2M applications are Information-Centric and rely on a publish/subscribe service model. Accordingly, in [42] has been proposed an ICN-based communication framework for M2M networks with resource constrained devices.

Because of the large number of nodes, scalability of MAC protocols is one of the essential components of M2M communication. Also, environment mobility, because of the elimination and addition of nodes, is another characteristic of M2M communications. Compatibility with changing number of nodes alongside with low control overhead is very important in M2M. Proper wireless protocols for physical layer in wireless communication, which are useable in M2M communication model, are generally divided into three main groups: Contention-Free MAC Protocols, Contention-Based MAC Protocols, and Hybrid MAC Protocols. Disadvantages of contention-based protocols in M2M communications are: Lack of scalability, low throughput, high power consumption, overhead of control packets, channel eavesdropping, and delay in real-time applications. The contention-free protocols have better efficiency in higher loads, but are not suitable for M2M networks that require high flexibility and scalability. Hybrid model combines the advantages of both mentioned methods for low and high loads [2]. On the other hand, cognitive radio technology is very promising in realizing the M2M communications for Internet of Things. In this regard, [43] has used the cognitive radio technology on protocol stack for M2M networks.

2.4. Routing

IoT technology consists of devices which are connected and embedded in all types of things. So, there is need for routing protocols to connect heterogeneous things together. In (RFC 5826), (RFC 5548), and (RFC 5867), routing requirements in different scenarios of home automation, urban Low power and Lossy Networks (LLNs), and building automation have been introduced and discussed. Routing protocol is an example of network layer protocols that provides end-to-end message delivery services. Some of the presented routing protocols in IoT are [1]:

- IPv6 over low power wireless personal area networks (6LoWPAN) is an IPv6 adaptation layer so that IP connectivity over low power and lossy networks is possible by this protocol [33], [44].
- Routing protocol for low power and lossy networks (RPL) is developed as a proper routing protocol for LLNs [9], [43]. Because routing operations in 6LoWPAN are very challenging due to the nature of nodes in resource constraint. RPL is a reference standard for IoT applications which are compatible with IPv6.
- IPv6 over the time slotted channel hopping mode of IEEE 802.15. 4e (6TiSCH) is based on IPv6 and be used over wireless mesh networks of IEEE 802.15.4e TiSCH. This protocol contains of details about packets, security, link management, neighbor discovery and routing.

With the increasing of the number of wireless devices, MAC sub-layer protocols and new routing protocols have been developed to guarantee the efficiency of end-to-end networks. As it is mentioned in [5], the existence of a mathematical model in MAC protocols of sensor networks is very important and it has been supported in [45]-[47]. In addition, the important effect of MAC parameters on the performance of IEEE 802.15.4 networks has been discussed in [45]. In [46] a Markov chain model has been used to design a distributed adaptive algorithm. Also, in [47] has been presented a mechanism for automatic selection of MAC protocol.

In order to prevent traffic congestion in network center, [9] has introduced a Content-Centric Routing technology called CCR, the aim of which is to store and share data based on the content. Thus, CCR can increase network lifetime, decrease network delay and can also improve reliability of communications significantly.

In IoT networks, secure routing plays a fundamental role in integrated and safe performance of the whole network. According to [48], [49], finding a general, proper, and practical solution for all routing attacks in IoT nodes is an unsolvable problem. So, in [1], secure routing protocols in IoT networks have been analyzed. It shows conventional routing protocols in Internet of Things (RPL and 6LoWPAN) lack the proper security implementation, and therefore, different security techniques such as key management, encryption, and trust management have been applied in [1]. Also, in [50], a routing protocol for Emergency Response IoT based on Global Information Decision (ERGID) has been presented which aims to improve performance of reliable data transmitting, and to have an efficient reaction in emergency conditions of IoT. A summary of articles classification in communication domain has been shown in Table III.

3. Trust Management

Since virtual communications expand, one of the best solutions to make pervasive the emerging system of IoT is vulnerabilities resolution and upgrade security level in IoT.

Based on what [11] says, all topics such as security (confidentiality, integrity, availability), privacy-preservation, dependability (reliability, safety, …) and etc, are considered as a part of the large scope of trust management. Therefore, we considered trust as the main area and the concepts discussed above as subareas. Now, since in the most of studied papers in trust domain, discussions have been assigned to the three cases; security, privacy-preservation and reliability, and other topics have been less discussed. So, continuation of discussion is dedicated to three subareas: security, privacy-preservation and reliability.

TABLE III. Classification of Communication Domain Papers

IoT Domain	Sub-domain	Research Field	References (Papers)
Communication	Standardization		[6] [21]
	Protocols		[31] [32] [33] [34] [35] [36] [37] [38]
	M2M	MAC Layer Protocols & Issues	[2]
		Mobile M2M Computation	[40]
		ICN-based M2M Communication	[42]
		Cognitive Radio Communication	[43]
	Routing	Secure Routing	[1]
		Content Centric Routing	[9]
		Routing Specific Protocols (RPL & 6LoWPAN)	[33] [43] [44]
		MAC aware Routing	[5]
		Routing protocol for emergency response IoT	[50]

3.1. Security

According to [51], security requirements based on the existing potential security threats and also the papers, which are related to this field, are divided into two main categories:

1) Authentication and Confidentiality

One of the important studies in this field is [52] done in 2014 and [53], [54] were also presented in the next years to improve it. In these papers, an Authentication Key Agreement Protocol (AKA Protocol) has been presented, that enabled owner of smart card to do the authentication process remotely and of course safe, through only one sensor. This process was performed in four phases indirectly on the gateway. In addition, to save time and energy in the same phase of authentication, key agreement process was also performed for the agreement of two ends (Sensor and User) on one shared session key.

In [55] a group-based AKA protocol has been presented to increase security level in M2M communications of LTE networks. In this protocol, Authentication and Key agreement process has been implemented in a distributed manner such that the solution will update a group of security policies for nodes.

2) Access Control

In this category of papers, the main purpose is certainly to focus on the access control and to determine individuals or nodes permissions, which are essential to keep everything secured. In [56] the access control of internet users has been investigated while they were querying of WSN sensors and it has used a new scheme named heterogeneous signcryption. Purpose of the signcryption is the scheme that does digital signature and public key cryptography operations in one logical step. This work leads to reducing energy in WSN environment.

In [57] some strategies have been included to control the access of guest devices and network applications to network resources. In this article, a token-based encryption mechanism has been used to grant permission to these devices. In [58], a new safe mechanism has been presented to guarantee the process of data source authentication & authorization in MQTT protocol.

3.2. Privacy

It is required for privacy-preservation that users be able to control personal data in such a way that they can determine "what information, when, and how to be communicated with others?" [59]. RFID systems have serious problems related to security and privacy. For example, in [60] to keep fix the authentication time, a shared master key has been used for all tags, which increases the vulnerability of the system from the privacy point of view. In [34], although a shared master key has been used for all tags, it has used safe memories of PUF (Physical Unclonable Function) in order to upgrade privacy level. Using this type of storage is to include required strategies against the enemy attempts in channel which is done to access the master key.

In [59] an application for smart parking has been presented that aims to increase privacy preservation level of users based on the two valuable achievements. First of all, this application operates independently than platform and Operating System (OS), and also, is scalable and efficient. Second, and more important, this application avoids private and personal information exchanging (like work and home address) under unsafe wireless network. In the application, ECC (Elliptic Curve Cryptography) has been used to do the public key cryptography. In [61], all risks that threaten privacy preservation in designing automated smart homes have been studied.

3.3. Reliability

If reliability be considered as the probability that data packets are received successfully by the receiver [62], so design this parameter will need to transition from a deterministic to a probabilistic process [63].

In order to increase reliability in industrial WSN [62] has used a hybrid protocol, which consists of ARQ SW protocol (with high reliability and high delay around sink node), and NCRT protocol (with low delay and high energy consumption far from sink node). Therefore, in this hybrid protocol, reliability has reached its maximum level, and the network delay will be less and network lifetime will be longer.

In [64] in order to increase reliability first, the reliability of all network terminals in wireless networks with limited links has been investigated. Then, a fault tolerance method has been suggested, in which there are redundant radio modules for each node.

It must be considered that since M2M communication are used widely in many IoT applications, reliable M2M communication is one of the IoT performance evaluation criterias. In such conditions, with mass volumes of M2M devices deployment in cellular networks,

TABLE IV. Classification of Trust Management Domain Papers

IoT Domain	Sub-domain	Sub Area Concepts	Research Field	References (Papers)
Trust Management	**Security**	**Authentication**	AKA Protocol for IoT-Based WSN	[53] [54]
			Group-Based (Distributed) AKA Protocol for M2M in LTE Net.	[55]
		Access Control	Identity-based Access control for heterogeneous IOT environment	[56]
			Temporary & conditional access control	[57]
			Guarantee Access control in MQTT	[58]
	Privacy	–	Privacy-Preservation for smart application	[59]
			Privacy-Preservation for automation smart home	[61]
	Reliability	–	Reliability in wireless net by a fault tolerant method	[64]
			Reliability for M2M communication in Cellular network	[65]

reliability upgrade seems absolutely necessary in such networks [65]. Accordingly in [65], in order to upgrade reliability of communication among the M2M devices and eNB devices, a set of schemes for coding in shared networks using Fountain method, has been presented. A summary of classification of trust management papers has been shown in Table IV.

Our studies in IoT trust management domain are an analysis of security challenges and issues of middlewares, platforms, or applications of IoT that each of them are usually related to a specific application [58] and a few works like [34], [59], [60] which are discussed earlier, are theoretical works and their designs have been done independent of specific application and environment.

4. Technology

As we know, the emerging paradigm of IoT is a new innovative achievement that is a combination of various technologies which are divided into two main categories: Enabling Technologies and Supportive Technologies that the following is the reason of this categorization. Our deeply research on IoT papers shows that enabling technologies like RFID and WSN are technologies which are necessary to integrate together in order to reality realize the concept of IoT, so the establishment of IoT will be literally meaningless without collaboration of these technologies. About second category like cloud computing, grid and so on, we can say the presence of these types of technologies is not mandatory and necessary for IoT establishment and deployment; but they somehow support IoT so that, the aim of applying them is upgrade and improve IoT performance.

4.1. Enabling Technologies

Examples of this type of technologies are following cases:

1) RFID

The emerging paradigm of IoT is a network that consists of things (human, animal, or any type of everyday physical things [13]), each of them has a unique identification. Therefore, RFID systems are proper solutions for assigning these identifications to things [34]. RFID systems, alongside with WSN technology, have been the first infrastructure of IoT environment. The main goals of the cooperation of these two types of technologies are to sense, identify, and to track things [13]. Despite the fact that RFID systems have more usage in IoT, unfortunately the most important problem of using these systems is privacy issue. The major reason for such issue is that stored data in RFID tags which are embedded in all of the everyday and personal devices of individuals, can be accessible by every reader [13], [66]. This means that privacy of individuals is violated which arise the question of "Who will control these collected data?" for the users of such systems.

- In [66], an appropriate protocol has been proposed in order to enable to control existing data in object tags by the owner of the object as the only legal operator. In this article the concept of RFID systems of key-evolving is recognized.
- In [34], in order to improve privacy in RFID systems, an authentication protocol has been suggested, which unlike previous cases, have been designed for large scale RFID systems.

2) Wireless Sensor Network (WSN)

Wireless Sensor Networks (WSN) consist of a number of sensor nodes with the capability of receiving information from the environment, and transmitting them to the neighbor sensors with limited processing capability and limited energy. These types of networks are widely applied because of having capabilities of low costs, scalability, trust, accuracy, flexibility, and simple development [67]. Parameters such as variety and heterogeneity of nodes [68], QoS [69], security [70], and scalability [67] are considered as the challenges of wireless sensor networks. Since WSN is one of the main and important components of IoT concept, therefore, these challenges are significant in Internet of Things. The sensor network area has affected some technologies and has been affected by them as well, creating a type of synergy.

4.2. Supportive Technologies

There are several types of these technologies that include: cloud computing, web technology, Software Defined Network (SDN), grid, crowdsourcing, fog computing, Cyber-Physical System (CPS), distributed computing, and Information-Centric Networking (ICN). Some of the most important and applicable types are discussed in following.

1) Cloud Computing

According to the resource-constraint of IoT devices in terms of processing, battery, and memory especially when storing and processing of acquired data (have time and space complexities) are costly tasks, transmitting data to another space seem to be necessary and logical. Cloud can be a proper infrastructure that can resolve the problem, and to support IoT [71]. Cloud platform collaborates and supports IoT which can be classified into four main categories [14]:

- Cloud-based Middleware for IoT

In [26] a cloud-based middleware has been designed and implemented for mobile crowdsensing, which has capabilities including: selected acquisition of sensors data, which are aggregated and filtered, and then sending these pre-processed data to cloud for efficient processing, and sending delivery-notification for mobile devices in real-time.

- Cloud-based Architecture for IoT

One of the major challenges in developing smart applications is to integrate sensors and devices automatically, and to provide data in service format to application layer [72]. In [73] the integration has been developed by network sensor, and in [72] the scenario has been developed in form of cloud-sensor, which has four layers architecture under the cloud platform. Automated integration of sensors in lower layers causes data, in form of various services, to be transmitted to the highest layer (cloud), where applications are developed and deployed.

- Cloud-based Platform for IoT

Cloud technology has high potential in designing platforms like e-health that needs to accurate, secure and real time processing of big data [74]. Therefore, in [74] a platform has been presented that supports medical information in three layers architecture. In this platform if anomaly occurs or be detected in collected information in cloud, all necessary actions will be done in real-time. Another similar related work is designing cloud-based platform for smart wheelchairs in order to facilitate disabled people problems [75].

- Cloud-based Framework for IoT

In [76] a hybrid framework named Calvin has been introduced which has applied new methods in order to facilitate development and to manage all mentioned software in above. The main advantage of this framework, from the developers' viewpoint, is that there is no need to worry about communication protocols and data transmission details.

2) Information-Centric Networking (ICN)

Due to universal development of internet and increasing the massive volume of network traffics, distributing and repeating content are inevitable in order to preserve system scalability [77]. In fact, what is done practically in ICN is that it uses in-network storage for caching effectively and multiparty communication for replication [78]. Also, ICN is able to direct network architecture evolution from IP-based towards content-based [79] in a way that assigns to each content a unique and persistent name, which is useable by router directly [42].

All the works conducted on ICN in IoT are mostly related to the suggested various architectures under ICN, and consist of following cases:

- Data-Oriented Network Architecture
- Content-Centric Networking (CCN)
- Publish-Subscribe Internet Routing Paradigm (PSIRP)
- Network of Information (NetInfo)

Explanation of few papers has been mentioned in the following.

The focus of CCN architecture, which proposed in 2007, and NDN (Named Data Networking) project that presented in 2010 [80], was on caching and providing a suitable method for CCR [9]. Since one of the common problems in IoT-based WSN is high traffic congestion in nodes, which are close to access point/server, researchers in [81] have suggested a proper approach for routing data based on their content. By this solution, first data aggregation does in similar nodes, and then a summary of data is sent to neck node. By eliminating redundant data transmission, energy consumption, traffic and delay are reduced in network.

After improving CCR in [9], this routing solution has been improved and developed in a way that nodes transmit data towards similar nodes that are capable of processing and aggregation. They transmit data by choosing reliable links, so traffic and energy consumption is reduce by using a distributed and content-centric routing method and also by data aggregation.

3) Software Defined Network (SDN)

With development and growth of networks [82] and also increasing of the heterogeneity amount because of the variety of equipment, different programs of various developers, more complicated management, and numerous human errors [83], has been increased the complexity of computer networks. Software Defined Network (SDN) technology has a new and centralized view at the network performance, the result of which is better and more efficient management of computer networks. This is done by separating the control operations from data exchanging inside the routers [84].

Among the introduced technologies for future networks, like NDN networks and programmable networks, the SDN technology is more effective than other networks. This type of technology suggests various solutions for virtualization and security. Also, it provides capability of testability and simultaneous work on new idea in networks are working [84]. In traditional networks, routers direct data and control the operations in distributed form. Whereas, in SDN network the tasks are separated and control section has programming capability [85]. The applications of SDN in IoT, is reviewed in some articles including the following cases: suggesting a framework for IoT [86], scalable communication method [87], and proper sensing mechanism [88].

4) Fog Computing

Services that are sensitive to delay and also mission critical services need to real time response with high processing capability. These cases are not suitable for communication with cloud in remote distances and through internet. Thus, fog computing plays a important role in this regard, and reduces distance by bringing resources near the edge (IoT devices). It also creates an interface network between this network and cloud and so provides concept of cloud beside the network. Fog computing model plays the role of a smaller data center which has more processing power and more storage, near IoT devices. Yet, no standard has been presented for resource management in fog computing.

Cloud environment is suitable for centralized applications and fog environment is suitable for distributed applications. Fog framework with high computing capability and storage capacity provides cloud services near IoT devices. Environments with movable things, applications with low delay, smart communications, context-aware computing, as well as more powerful and more intelligent gateways are all achievements of using the fog's storage capacity and processing power.

The main difference between fog and cloud is in their local and global accessibility respectively. Also, fog service level is local, and cloud service level is global. Fog computing provides security for sensitive data, and it also has easier accessibility [89]. Ref [90] provides a security framework for smart applications in IoT. All categories in technology domain have been shown in Table V.

5. *Resource Management*

IoT consists of various nodes with various resource capacities. The choice and supplying of resources will affect the QoS of IoT applications greatly. Resource management is very important issue in distributed systems. So, dynamic and heterogeneous nature of resources in IoT has challenged resource management in Internet of Things. An efficient resource management needs to stability, fault tolerance, scalability, energy efficiency, QoS, and Service-Level Agreement (SLA) significantly. In [22], resource management for IoT environments includes:

- Partitioning resources
- Discovering all available resources and services
- Scheduling tasks on the available physical resources
- Code offloading (computation offloading) which is used to transfer specific computing tasks to the external platforms.

According to this cases, can be resulted that the aim of resource management methods is to improve QoS. Therefore in this paper, in addition to the above, quality of service is also considered as one of the resource management sub-domains.

5.1. *Resource Partitioning*

The first step to satisfy IoT needs for resources is to partition them effectively and to reach a high utilization ratio.

TABLE V. Classification of Technology Domain Papers

IoT Domain	Sub-domain	Sub Area Concepts	Research Field	References (Papers)
Technology	Enabling Technologies	WSN	Security services	[70]
			Efficient Management & Optimization	[68] [69] [91]
		RFID	RFID System Privacy	[66] [34]
			Automatic RFID Monitoring System	[92] [93]
	Supportive Technologies	Cloud	Cloud-Based Middleware	[26]
			Cloud-Based Architecture	[72]
			Cloud-Based Platform	[74] [75]
			Cloud-Based Framework	[76]
		Software-defined networking (SDN)	Framework	[86] [87]
			Sensing	[88]
		Information Centric Network (ICN)	Content-centric	[9] [94]
			Name-centric	[42] [95]
		Fog Computing	Framework	[90]

This idea is widely applied to cloud computing through virtualization techniques and suitable infrastructures [22]. Since hypervisor is responsible for the interaction management between the host and the guest of the virtual machines, therefore it needs a significant amount of memory and computational capacity. Consequently, mentioned configuration is not appropriate for Internet of Things, because most devices in IoT have the limited memory and processing power. In order to address the challenges, the concept of container has been arised which it refers to virtualization technology and is adaptive with the request of resource constrained devices. In this regard, [96] is a survey paper which has also studied the centralized virtualization techniques for embedded systems in real-time applications. In [97] has been used the virtualization with container technologies for Edge-IoT scenarios in which devices have constrained resource and low-power. [98] introduces a new IoT virtual framework based on Sensor-as-a-Service which aims to maximize the sensor performance.

5.2. Resource/Service Discovery

The current architectures for IoT are not a standard and efficient method for service discovery, combination and integrating them in a scalable way. Discovery in IoT environments has two parts. First step is to identify and locate physical devices and second target is to discover desired service which should be used [22].

Efficient algorithms which choose dynamically centralized or flooding strategies can minimize energy consumption, although due to IoT dynamic nature, other parameters like mobility and delay should be considered in order to suggest a proper solution in IoT [99]. In [100], also has been used a hybrid architecture for resource discovery that combines the features of both centralized and distributed methods. The aim of this solution is discovery of available resources in a scalable and efficient manner. In another method based on fog computing [101], available resources such as network bandwidth, computational criterias and storage capacity have been converted into time resources, which aim to facilitate resource sharing. [95] introduced a contextual IoT service discovery scheme based on NDN, which is a proper solution for Information Centric Networks.

5.3. Scheduling

OpenIoT scheduler has capability of availability and preparation of exact information about the needed data by every service. So, wide scope of different algorithms for resource management and optimization can be implemented at the openIoT scheduler [22]. Some reviewed papers related to scheduling sub-domain as follows:

In order to support uplink-heavy traffic that is generated by M2M communication, [102] presented a new LTE uplink packet scheduler. This solution satisfies the QoS requirements and ensures fair allocation of resource. Also, [103] proposed an IoT uplink multiple-input and multiple-output (MIMO) scheduling scheme for multi-user (MU) in IoT-gateway devices to greatly extend the uplink bandwidth and deliver huge data to gateway. [104] is a research work about dynamic scheduling for cloud computing, which is an approach based on priority of IoT requests to provide desired services. In [105] by clustering things/sensors into IoT subgroups, a message scheduling algorithm with efficient energy in the IoT system has been presented in which failure issue has been considered.

5.4. Computation Offloading

Code/Computation offloading is a solution to investigate the constraint of available resources in mobile and smart devices. Some advantages of computation offloading are efficient power management, fewer storage, and higher performance of applications. However, offloading technique still faces many challenges related to practical usage. According to what has been mentioned in [22], most of the code offloading techniques will use the static code analyzers and dynamic code parsers, if there are network fluctuations and high latency [106]. In this regard, [107], [108] used virtual machines instead of physical samples to increase scalability and elasticity.

In [109], Mobile Cloud (MC) and IoT have been merged in distributed environments to design a new method of computation offloading in MCIoT platform for mobile and portable devices. To do so, a new model of nested game theory has been presented. The main goal of this model is to maximize the performance of the mobile device, also to provide QoS. In [110], also has been identified the challenges and issues related to code offloading for mobile cloud. Then, an approach for a general code offloading architecture has been proposed to reduce the limitations. Recently combining cellular networks (mobile phones) and IoT has created a new platform of services for all types of traffic applications. Therefore, in [111], a new scheme of traffic control has been presented based on data offloading method.

5.5. Quality of Service

Knowing challenges that IoT probably faces, lead to provide high quality services by service providers. Some of these important challenges are: accessibility, reliability, mobility, efficiency, scalability, interoperability, security, trust and management. Also, by improving mentioned parameters in network, the quality of given services increases [6].

The large number of things, and also heterogeneity of things and networks make it complicated to provide QoS. Since resources are constrained and applications are various, new methods for providing services with quality are necessary. Common parameters related to quality of service are not enough for IoT and there are more requirements because of applications and characteristics. A solution for providing QoS is service based three layers architecture and that means the providing quality of service at application, network and infrastructure layers [112].

QoS parameters at application and network layers are similar to mentioned cases in conventional networks, but these parameters in infrastructure layer are different than traditional networks. In the application layer, [113] presents a lightweight method to simplify management, as well as [114] increase reliability in traffic congestion and decrease delay. In delay field, [115]-[117] have attempted to decrease delay and time of events detection. In addition, location-based components in RFID systems are investigated in [118], and [91] is about query optimization in WSN for industrial IoT applications. Table VI shows a summary of classified articles in resource management area.

6. Energy Management

As previously mentioned, IoT devices are energy constrained. Also growth of number and types of these devices has caused the energy demand in IoT applications be increased. So, one of the basic IoT challenges is interoperable connection of things together according the limitations of energy and high energy consumption of devices while they are communicating. Consequently, energy management is considered as a critical issue in order to development of low power technologies and improvement of battery efficiency. In this regard, there are solutions based on Radio Frequency (RF) and Energy Harvesting (EH) [119]. The RF solution is used because of need for integration and low power consumption that have been released in wide range of applications in IoT. Also, EH method is a proper solution for extending the lifetime of low power devices. Therefore, based on [119], energy management domain has been classified into two sub-domains, which are discussed in more detail in the following subsections.

6.1. Low Power Communication

Standardization institutions have suggested low power communication technologies which some of them are following [119], [120]:

- IEEE 802.15.4 is a standard to decrease cost, power consumption, and complexity which has been developed for resource constrained devices at physical and data link layers.
- Bluetooth Low Energy (BLE) is a power-conserving variant of wireless personal area network (PAN) technology, with more than 15 times efficiency in comparison with Bluetooth.
- Ultra-Wide Bandwidth technology (UWB) is a type of technology in which signal transmits in a much larger frequency range than conventional systems.
- ISO 18000-7 DASH7 is a low power standard with low complexity and a radio protocol for all radio devices sub 1GHz.
- RFID/NFC proposes different standards for contactless methods.

The front-end architecture is traditional, and requires innovation. In order to achieve ultra-low power consumption, super-regenerative architectures are very suitable and efficient for wake-up receivers [120]. In this regard, [32] has suggested a solution to further reduce the energy consumption of BLE in a home automation (smart city). To do so, it is used a fuzzy logic based mechanism by determining the sleeping time of devices. Also, to meet the challenges in smart cities, [121] has proposed an energy-efficient

TABLE VI. Classification of Resource Management Domain Papers

IoT Domain	Sub-domain	Research Field	References (Papers)
Resource Management	Resource Partitioning	Virtualization Framework based on Sensor-as-a-Service	[98]
		Container Virtualization	[97]
	Service/Resource Discovery	Mobile Cloud Computing	[99]
		Hybrid CoAP-based discovery	[100]
		Contextual Service Discovery in ICN	[95]
	Scheduling	QoS-aware LTE Uplink Scheduling	[102]
		Uplink Scheduling for MU-MIMO Gateway	[103]
		Cloud Computing	[104]
	Computation Offloading	Mobile Cloud Computing	[109] [110]
		Traffic Control	[111]
	Quality of Service	Lightweight Management	[113]
		Reliability	[114]
		Delay	[114] [115] [116] [117]
		Accuracy (for location)	[118]
		Query Optimization	[91]

scheme based on dynamic traffic demands.

Recent advancements of CMOS technology haveresultednewparadigmsinRFcommunication. Applications which require RF connectivity are developed alongside with IoT technology, and are suggested as stable and economic solution. According to RF architectures, RF characteristics could be added simply to the developing existing devices which results in applying digital blocks versus analog blocks. Thus, receiver architecture should be has the same required performance to digitize signals effectively. In this regard, it is suggested that band-pass sampling get done at much lower frequency than Nyquist ratio [122]. Consequently, energy consumption decreases significantly by using this method. Moreover, in order to have digital and portable RF solutions, continuous-time quantization is an appropriate method for portability and compatibility. Thus, energy consumption is considered regarding signal level and independent of time [120].

It is to be mentioned that cable devices are not appropriate options for IoT devices because they have high costs for development. In many cases, replacing device battery to set up and develop of IoT scenarios is impractical or very expensive. Therefore, to extend IoT in large and independent scale, use of alternative energy sources or ambient energy should be considered [120]. IoT applications need a lot of wireless terminals solutions that consume low power. For this purpose, [123] has introduced a new microcontroller cheep of Bluetooth smart with adaptable RF technology as RF/BLE that minimizes power consumption using the RF circuit technologies. Also, in [124] is presented a low power radio receiver dedicated to lower GHz frequencies in which sampling frequency fixes the carrier frequency of the received signal.

6.2. Energy Harvesting

In this technology, small but usable amount of electrical energy is collected from the environment. Some researches about energy harvesting focus on acquired changes of external temperature, sound, environment vibration, and environment RF. Unlike the previous RFIDs, in modern systems an energy harvesting converter produces required electrical energy for a microcontroller, sensor, and a part or whole of the network interface [125]. From the technical aspect, energy harvesting converter reacts not only to external resources, but also to any type of power intentional transmissions for example through the voice channel and RF.

Ambient energy sources that are available in the environment as follows: mechanical energy (deformations, vibrations), thermal energy (temperature gradients or variations), radiant energy (RF, infrared, sun), and chemical energy (biochemistry, chemistry). Energy Harvesting (EH) method should be chosen considering local environment. For outdoor or bright and sunny indoors, solar energy harvesting is the best solution. In closed environments where enough light

don't exist, mechanical energy or thermal energy is a proper choice. Generally the amount of the power of the initial energy source which is used to produce electrical output power in desired environment is considered as harvesting energy [120].

In the last decade, there have been significant changes and developments. Thus, many researches are conducted about energy harvesting, so that most of the present technologies advancements should satisfy the IoT needs. Some of the related articles have been reviewed in the following.

The purpose of decreasing energy consumption from environmental aspect is to minimize greenhouse gases released. It is possible in Information and Communication Technology (ICT) industry by using renewable energies. In [126], first indexes are studied that show the effect of ICT technology in energy consumption from data center to WSNs. Then, it has mentioned some of the recent research works for each layer in internet protocol stack, from physical layer to application layer, which involves in energy efficiency, or in other words, green communication.

Among the various energy harvesting methods such as vibration, light, and thermal energy extraction, it is proved Wireless Energy Harvesting (WEH) is one of the most appropriate solutions. In [10] those technologies and designs have been investigated that activates WEH for the Internet of Things systems. There are various wireless devices for energy harvesting that will provide services as the IoT fundamental and forming blocks.

In [127], kinetic (motion) energy availability has been discussed for IoT applications in which the optimal energy allocation algorithms are designed and their performance is evaluated. Ref [128] introduces an idea to achieve photovoltaic energy harvesting system with high efficiency. Energy scavenging from photovoltaic (PV) cells is one of the practical and applicable solutions from viewpoint of power density among the existing energy harvesting resources. For this purpose, PV power systems allow the Maximum Power Point Tracking (MPPT) in order to scavenge maximum amount of solar energy. As it is come in Table VII, can be observed classification of all studies related to energy management.

7. Soft ware Services

Internet of things is an interconnected network of smart, unique, and identifiable things. These infrastructures make the required backbone for most of the applications that require the connection between the components. Our studies on papers of this section show that IoT software services domain is very wide, from smart applications to some services, APIs, operating systems (OS) and software platforms, but we focused on smart applications and services as two subsections that high percentage of the papers were about them. So, this section of the paper has two subsections, which first involves the smart IoT applications, and then it discuses services.

7.1. Smart Applications

The purpose of smart applications in IoT, is to help the daily life improvement of human and entire society. Gascon and Asin, in an extended study, have classified different IoT applications into twelve main categories which each of them contains a collection of various applications. These categories are: smart environment, smart city, smart metering, smart water, security and emergencies, retail, logistics, industrial control, smart agriculture, smart animal farming, domestic and home automation, and e-health (Sensor Applications). Also, Kim et al. have done a study and research related to IoT applications based on software services domain, and with the aim of user groups [129]. Many researches have been done in the field of smart applications including Health care [93], [130], Industrial applications [131] and Smart City [132].

The Beecham Research institution is also involved in marketing field. This company has defined four layers for M2M market which are: service sectors, application groups, locations, and devices. Each of these four layers has been divided into several segments, which contain of different IoT applications. For example, service sectors layer has nine key applications as follows: IT and networks, security/public

safety, retail, transportation, industrial, healthcare and life science, consumer and home, energy, and building (M2M Connected Services).

7.2. Service

In accordance with [6], IoT services can be generally classified into four classes [133], [134] which are as follows:

- Identity-related Services are the most important and fundamental services which are used in other services. In every application that

TABLE VII. Classification of Energy Management Domain Papers

IoT Domain	Sub-domain	Research Field	References (Papers)
Energy Management	Low power Communications	Low Power Technology (BLE) in IoT	[32]
		Energy Efficiency based on Traffic Pattern	[121]
		RF-solutions for IoT applications	[123] [124]
	Energy Harvesting	Energy-Efficient Approaches for the Internet Protocol Stack	[126]
		Wireless Energy Harvesting (WEH)	[10]
		Kinetic Energy Harvesting	[127]
		Storage-less and Converter-less Photovoltaic Energy Harvesting	[128]

needs to be transferred physical things to virtual world, these services should identify the things identity.

- Information Aggregation Services collect and aggregate the unprocessed information which need for processing and reporting to IoT application.
- Collaborative-Aware Services act higher than information aggregation services, so that they can use obtained information to make decision, and consequently, react.
- Ubiquitous Services that purpose of such services is to provide collaborative-aware services at anytime, anywhere, by anyone who needs them.

The final purpose of all the IoT applications is to reach ubiquitous services level. However, this aim is not simply achieved because there are so many difficulties and challenges which need to be addressed them. Most of the existing applications provide the first three types of services in a way that smart health-care and smart grid are in service category of information aggregation as well as smart home, smart buildings, intelligent transportation systems, and industrial automation are closer to collaborative-aware services category.

It is to be mentioned that in classifying the studied articles, most of software discussions such as software platforms (including OS and programming), APIs, frameworks and similar cases [135]-[137] are considered as service sub-domain. Related papers to software services classification have been shown in Table VIII.

8. Data Stream

In IoT network, different things are generating continuously huge volume of heterogeneous multidimensional data which based on definitions are data streams [138]. While IoT data streams are considered as a generation resource of big data, so the challenges and issues of this section might be similar with challenges and issues of big data. According to [139], these challenges are divided into four groups:

- data stream processing
- complex event processing
- storage models
- search techniques

Which are related pairwise:

1) Data stream processing → 2) Complex event processing
3) Storage models → 4) Search techniques

In data stream processing, the goal is to find the most valuable techniques to do analysis, aggregation, mining and result in valuable patterns or knowledge discovery, while complex event processing (CEP) is based on data stream processing and data stream is seen in the format of a collection of events that have occurred in environment and the goal is to filter and compose of them and transform the result to high level events [139]. Therefore, CEP has higher level both in terms of operational complexity and abstraction level.

Due to the data structure in IoT Data Streams, new architectures and solutions are required in designing storage at different levels (thing,

TABLE VIII. Classification of Software Services Domain Papers

IoT Domain	Sub-domain	Research Field	References (Papers)
Software Services	Smart Applications	Smart Applications	[22]
		killer IoT application	[129]
		Health care	[93] [130]
		Industrial applications	[131]
		Smart City	[132]
	Service	Service Classification	[6]
		Operating System (Contiki OS)	[6] [135]
		Programming	[136] [137]

server and etc) to upgrade performance in store and restore processes. Also, one of the important problems in IoT data store is efficient techniques to search in these stored data streams in storages [139] that the efficiency of this techniques are directly related to storages designs. This discussion also includes the search for things. In the following, we will briefly describe the articles of the two first basic sections in data stream (data processing and CEP):

8.1. Data Stream Processing

Data stream processing can be done for several purposes including valuable patterns discovery to diagnose or prevent diseases, or RFID data analysis for stream cleaning, or stream compression to omit redundant data [139]. Our discussion be continued with the review of several articles in this field.

Mining on web traffic logs that contains valuable information, such as communication patterns between people and web services, or smart devices, will be very useful in different areas like network optimization and security management and etc [140]. In this regard, in [140] by applying web usage mining on user http requests, request dependency graph has been drawn. The sequences and dependency of web requests and user interests in graph will be used to optimize design of web applications and predict their needs. Similarly, in [141] recorded logs in ISP which contain information related to home devices M2M communications are studied and analyzed by data mining techniques like association rule mining, in order to discover the usage patterns of users.

In order to simplify data processing in IoT, it is better that acquired data from environment be aggregated, which can be considered as a phase of data preprocessing process [26]. To do so, in [142] a distributed service-oriented architecture has been presented in order to solve data aggregation problem in IoT industrial applications (IIOT). This architecture describes how distributed data of a product is aggregated with existing information in nodes.

8.2. Complex Event Processing (CEP)

In this type of data processing, data stream is seen in the format of a collection of events that have occurred in environment [139]. In CEP it is considerable that how these events are extracted which needs to implement and configure a set of rules in knowledge base, so that these rules be able to decide on events detection process [22]. CEP systems are used in many applications. In the following, briefly referred to two articles in this field:

In [117], a CEP system with new capabilities has been introduced that can be used in smart city. The system does operations in a distributed and parallel manner. Moreover, it has the capability of predicting the amount of its required buffer from the beginning (in previous-phase format); this amount is limited and unlike some similar systems does not need unlimited buffer. In addition, the system has used pattern-sensitive method for partitioning data flow.

Since the volume of generated data stream by RFID tags and sensors is high, it is impossible to analyze them manually. Therefore, the use of automated and accurate methods for doing such processes is necessary. One of the best and more efficient methods is to use machine learning algorithms, which are used as the rule-based classifiers in [143]. After performing data preprocessing steps, different solutions from rule-based classifiers are applied to detect complex events efficiently. A summary of article classification of data stream domain has been shown in Table IX.

9. Infrastructure/Hardware

According to [15] and based on majority of our review papers related to IoT infrastructure, in Internet of Things, the meaning of infrastructure layer is hardware layer which consists of various types of hardware from small things to routers and gateways that they provide necessary infrastructure for IoT implementation. So, in a more exact analysis, this domain is divided into two smaller sub-domains named resource type and device type. They are described in detail in the following.

9.1. Resource Type

In this type, IoT equipment is classified into two major categories of resource constrained devices, and resource unconstrained devices which can be considered as low-end and high-end respectively. The resource constraint includes memory, energy, and CPU capacity which affects

TABLE IX. Classification of Data Stream Domain Papers

IoT Domain	Sub-domain	Sub Area Concepts	Research Field	References (Papers)
Data Stream	Data Stream Processing	General Data Stream Processing	Association rule mining	[141]
			Web usage mining	[140]
		RFID Data Stream Processing	SOA Architecture for Aggregation	[142]
	Complex Event Processing (CEP)	Complex event processing	Distributed Parallel CEP	[117]
		Semantic Complex Event Processing	Rule-based Machine learning CEP	[143]

software and applications design. For example, memory constraint affects OS design, energy constraint affects interactions with devices and its activity, as well as CPU constraint affects determining application type (Constrained Devices). Also, in [144] has been referred to these constraints of the devices. Furthermore, TCP/IP protocol supporting capability is another criteria in classifying things [6].

According to (Constrained Devices), from the view point of available memory, resource constrained devices are classified into three main classes in IEEE standard. Class 0 consists of devices with very low resources that have memory much less than 100 KB. Class 1 consists of devices with medium level of resources which have about 10 KB RAM, and 100 KB flash memory. Class 2 contains devices with more resources but have much less resources in comparison with unconstrained devices.

Energy constrained devices are classified into four classes. Class E9 consists of devices that have no energy constraint. Class E2 consists of energy constrained devices, non-rechargeable, and their batteries are irreplaceable. Class E1 has constrained energy for a specific period of time, and they are chargeable or replaceable. Class E0 contains of energy constrained devices for a specific task. Because of the energy constraint, optimal consumption strategies are very important.

CPU-constrained devices are classified into five main levels. The first level consists of the smart sensors with processing power between 50-100 DMIPS. The second level is the sensors with about 1000 DMIPS processing power which has sound data processing capability. The third level has processing capability of video and sound flows. The fourth one has multi-core processors and 3D graphic processors. Also, the fifth level consists of powerful multi-core processors which have specific design and high efficiency to use resources efficiently (IoT Processors).

9.2. Device Type

Device type category consists of hardware which is used in network topology implementation, sense, and data aggregation, or operations like routing, communication, and also security issues. These devices can be categorized as following:

- Sensor (Processing Devices): The main component which forms IoT infrastructure consists of different types of sensors like temperature, humidity, and pressure sensors. Most of sensors have constrained resource. The responsibility of receiving environment information via sensors, and transmitting them are the most important tasks in this field.
- Gateway (Communication Devices): Considering high power of gateways compared to sensors, they do more tasks that sensors are not able to do. Because of the different requirements of sensors and variety of their communication standards, gateways should support different standards. Gateways are able to provide accessibility services by creating an abstract layer. This model improves horizontal development of various technologies. Gateways are classified into two smart and non-smart levels. Conventional tasks of non-smart gateways are protocol translation and things management. Whereas,

smart gateways are resource unconstrained, and have programming capability based on a set of rules. They can perform various processing, and by having powerful OS, they make possible all types of data processing. Smart gateways have different management facilities because of their programming capability (IoT gateway).

Gateways are classified into two categories from the viewpoint of code accessibility: industrial hardware (closed source) that depends on specific frameworks, and open source hardware that can be developed by users. Another model is based on programming capability and providing an abstract level for things [136]. In [145] has been introduced a WSN gateway framework for IoT named as WiSEGATE. It addresses end-to-end interconnection problem between several clients and sensor nodes.

- Storage Devices: Data in Internet of Things are very heterogeneous and are different than traditional internet data because they have time and location specifications. Things location changes dynamically during the time, and IoT data are multi-dimensional. An appropriate database model in IoT is very important because it can provide QoS parameters. OSD mechanism of data storage and processing provide the possibility of data maintenance and management in IoT by presenting a hierarchical model and more memory space and high processing power [146]. In [147] has been proposed a distributed IoT storage system which supports the capabilities such as flexibility, scalability and reliability at both data and system levels.

- Security Devices: Nowadays, different software programs and various hardware devices like Firewall, IDS, and etc have been used beside security protocols in TCP/IP protocol stack to preserve security in internet network [148]. This policy has been titled as "defense in depth" (Security Countermeasures). It seems that applying similar policies to preserve security in IoT, which is a network of interconnected things by the global internet network, has been a logical solution.

One of the most important security devices is Intrusion Detection Systems (IDSs). For the first time in [149], a distributed IDS both on the network and the node level was designed and implemented for IoT considering features and specific needs of this type of network. The IDS is presented under an appropriate architecture for ipv6 networks in IoT that use RPL protocol as the routing protocol in 6LoWPAN networks. It is also suitable to be used in resource-constraint nodes considering energy consumption. In the same year in [150] similarly a framework for IDS devices in IoT was designed which is ipv6 networks type based on 6LoWPAN devices. Other security device that is used in networks is firewall, the aim of which is to filter network packets to protect resources of internal network. To explain why this device is necessary in IoT network it can be said that despite all common security strategies, like authentication and encryption in IoT, this device can prevent attacks

TABLE X. Classification of Infrastructure/Hardware Domain Papers

IoT Domain	Sub-domain	Sub Area Concepts	Research Field	References (Papers)
Infrastructure/Hardware	Resource Type		Resource Constrained Devices	[144]
	Device Type	Communication Devices		[136] [145]
		Storage Devices		[146] [147]
		Security Devices		[148]
			IDS for IoT	[149] [150]
			Firewall for IoT	[151]

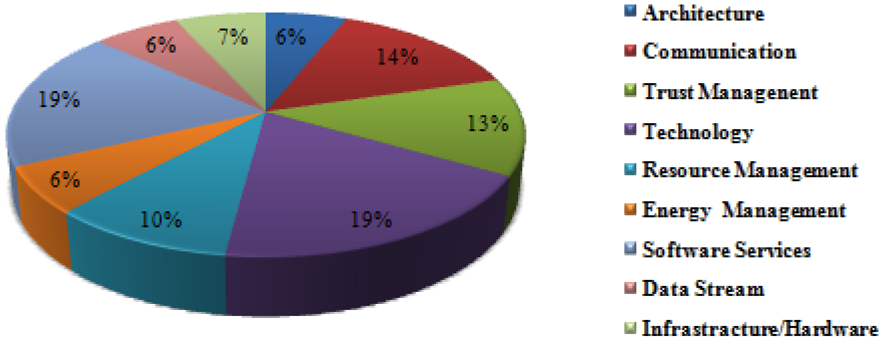

Fig. 3. Statistical Results of IoT Domains

or stop them before they start in the network (IoT Firewall). In [151], a standard approach has been presented to customize firewall for IoT network in smart homes. A summary of classification of infrastructure/hardware domain papers has been shown in Table X.

III. STATISTICAL ANALYSIS RESULTS

In this research, 339 papers of IEEE, Springer, Elsevier, and ACM publications in IoT area which have been published in recent two years (2015, 2016) have been investigated. The majority of our studied papers (60%) are published in 2015 and nearly 40% in 2016. Also the majority of them (52%) are published in IEEE publisher, 32% in Elsevier, %15 in Springer and the least of papers (1%) are published in ACM publisher. As it is seen, a high percentage of studied papers, about %99 of them, belong to Elsevier, Springer, and IEEE publications and only a small percentage, about %1, has been published by ACM. So, the obtained statistical results can be considered as a research trend of IEEE, Elsevier, and Springer publications in IoT area in the recent two years.

In our research, some papers are shared between some domains. For example, a paper which proposes new security architecture should be considered in both security domain and architecture domain. The purpose of these studies is to extract the area of activities precisely in order to present statistical results in each discussed domain and sub-domain. IoT trends in recent years could be useful for students and researchers who work in this field. In continuation of discussion, firs the statistical analysis results of main domains in IoT have come and then will be shown sub-domains statistical related to each of these domains separately.

The results of statistical analysis on IoT domains are shown in Fig. 3. As it is seen, studies and investigations show that the most of researches have been focused on technology and software services domains, each one with %19 of the whole statistical society in the recent two years.

Since the growth of information systems in IT in different abstract levels is for the purpose of satisfying needs of modern human life in the format of service, it may be said that what makes applications design and implementation (especially smart applications which cover a high percentage of papers related to software services (very important from the researchers and developers viewpoint, is to increase facilities and quality of life by relying on daily activities automation. Furthermore, it can be said about the technology domain, IoT paradigm is a combination of different existing technologies such as RFID, WSN and etc. Now, to increase the efficiency and performance of this network, various other supporting technologies have also been used. So, in short, it is obvious that the implementation and upgrade of this type of network without using mentioned technologies would be impossible.

1. Statistical Results in Sub-domains of Architecture

Statistical analysis and investigations show that a high percentage of researches conducted about the architecture domain (approximately %86) is related to architecture models sub-domain. Subsequently, service oriented architecture (SOA) has been attracted the attention of a large number of researchers in comparison with other presented architecture models. It has covered approximately %40 of the whole papers in mentioned sub-domain. The reason of this attention might be the popularity of SOA architecture in recent years and it's benefits like: service reuse, asset wrapping (ability to integrate existing assets) which will lead to reduce costs and time in system development and other benefits like: high level abstraction and service composition & discovery (SOA Features) which will lead to increase users facilitation and we know all of the mentioned benefits in SOA architecture are needed in IoT system. Statistical analysis results in architecture sub-domains have been shown in the diagram of Fig. 4.

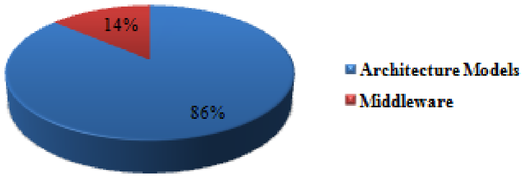

Fig. 4. Statistical Results of Architecture Sub-domains

2. Statistical Results in Sub-domains of Communication

Statistical analysis on communication domain papers show that M2M communication and protocols sub-domains (%38 and %37 respectively) have covered the major portion of the research works (Fig. 5). To introduce M2M communication importance in IoT, it can be said that one of the most important purposes of IoT network is to provide interconnection among machines without any need for human interactions. Such communication can play significant role in real-time monitoring applications, industry, health, smart homes and etc [65]. Also, our research show the IoT devices are resource constrained and specific limitations exist in this network in compared with traditional internet. Now, since the standard IoT protocols must be compatible with these conditions and limitations, it doesn't seem to be a logical choice to use protocols of traditional internet in IoT network. Thus to achieve communication efficiency in nodes and resources of network, it is necessary to design efficient and lightweight communication protocols in different layers of IoT protocol stack form different perspectives such as security and privacy preservation, low power consumption, optimized bandwidth allocation and so on.

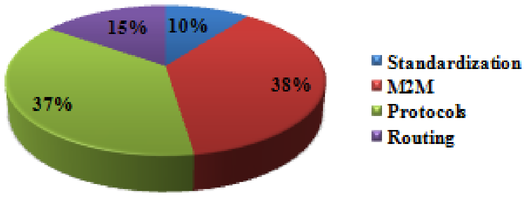

Fig. 5. Statistical Results of Communication Sub-domains

3. Statistical Results in Sub-domains of Trust Management

According to what has been shown in Fig. 6, the most of conducted studies in trust management area concentrated on security sub-domain. Considering that some IoT devices collect private information of people, their concerns about security and privacy preservation are indeed well justified. In such a situation, despite 68% of all trust domain papers focus on security sub-domain but this statistical results difference between security and privacy may not indicate decrement of privacy importance from the viewpoint of researchers and security community. But, since privacy is not achievable without security controls in data, communications, applications, device, and system level and indeed, the security primitives of confidentiality (encryption), integrity, authentication, non-repudiation, and data availability need to be implemented to support the overarching privacy goals for the deployment [152]. Therefore, it may be said that the security concept is necessary for research and challenge review at first as a basic building block of privacy concept.

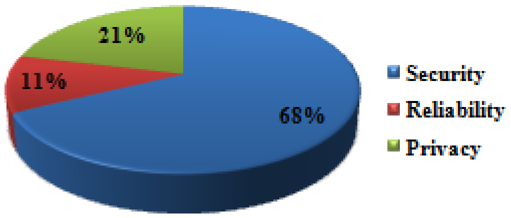

Fig. 6. Statistical Results of Trust Management Sub-domains

4. Statistical Results in Sub-domains of Technology

Statistical results of technology domain, which has been shown in upper section of the Fig. 7, indicates that there is an approximate similarity of research function rate in both enabling technologies sub-domain and supportive technologies sub-domain, which allocates %52 and %48 respectively, of all conducted researches in technology domain. In this regard, statistical results in sub-domains of enabling technologies, and supportive technologies, have been obtained through a hierarchical method (lower section of Fig. 7). According to these statistics, wireless sensor networks technology (WSN) with %72 in enabling technologies sub-domain, and cloud computing (as an essential infrastructure for information storage and processing) in supportive technologies sub-domain with %46 were the main subject of the most papers in the mentioned sub-domains.

We know sensors play an important role in the most of IoT equipment, from environment to individual and health-care things in order to monitor/control events of various environments or individuals states. So, obviously this field is one of the most important concepts in IoT and without this technology will not be met many of functionalities of IoT systems. On other hand, IoT as a resource of big data generation need to a platform which could store and process its huge data timely and accurately by providing the necessary quality of services requirements such as security and performance and so on. Since cloud as an appropriate platform could satisfy all of these requirements for IoT, in this situation, cloud has a significant role as a supportive technology compared to others.

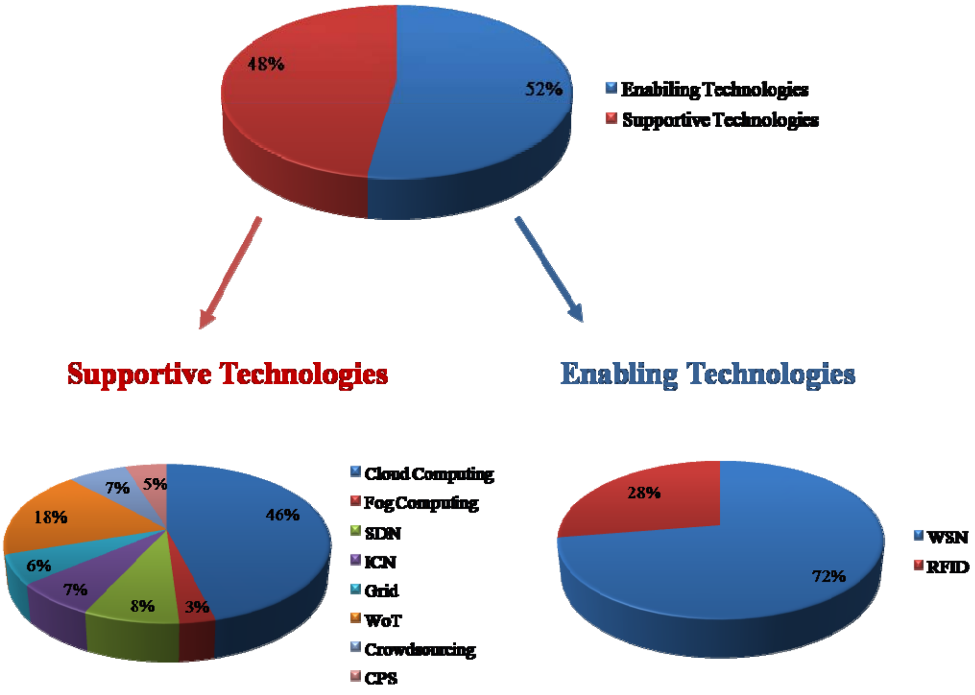

Fig. 7. Statistical Analysis of Sub-domains & Sub-subdomains of Technology

5. Statistical Results in Sub-domains of Resource Management

Analysis of the papers related to resource management domain indicates that most articles are focused on QoS sub-domain. According to what has been shown in Fig. 8, this statistic is approximately %59 of the whole papers of this collection. Maybe can be said that the reason for the importance of this sub-domain in this way that IoT development as a pervasive network needs to provide an appropriate quality level for the provided services. Whereas, providing such quality level in IoT has its own complexities and limitations because environment and data are heterogeneous. Therefore, to have an acceptable quality level in services, it is absolutely required to apply various mechanisms of QoS in different layers of IoT.

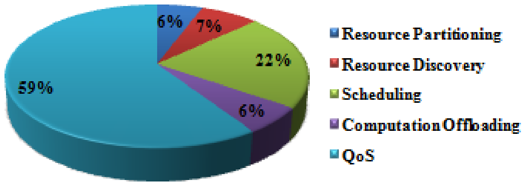

Fig. 8. Statistical Results of Resource Management Sub-domains

6. Statistical Results in Sub-domains of Energy Management

As it is mentioned in the previous sections of paper, although energy is considered as one of the existing resources,

but due to importance of energy management in order to optimize its consumption in IoT, is considered as a separate domain. As shown in Fig. 9, %81 of the all papers in this domain has been carried out on Low power communication sub-domain. Perhaps this difference in percentage is due to the fact that now what is more complex and unknown in IoT is how to consume energy optimally and cost effective by devices, and not how to can capture and store energy for these devices.

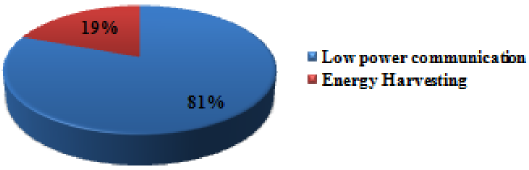

Fig. 9. Statistical Results of Energy Management Sub-domains

7. Statistical Results in Sub-domains of Software Services

As it was mentioned above, according to the statistical results of this research, software services is one of the domains which most of the studies related to IoT focused on it. In this domain, smart applications sub-domain with %55 allocates the maximum percentage of related studies (upper section of the Fig. 10). According to (Smart Applications) since 2010, the Global Innovation 1000 companies (collectively 40% of the world's total R&D spending) have increased their R&D spending on software offerings by 65% — to $142 billion. In fact, "R&D is shifting more and more toward developing software and services", and this shift is driven by the ever-increasing capabilities of software, the embedding of software and sensors in products, the ability to connect products via IoT and the cloud, and, as always, customer demand. So, it's manifesting in every kind of "smart" product and service.

Studies done on the smart applications papers show that smart healthcare with %25 has a major portion in designing smart applications (lower section of Fig. 10). Based on (R&D spending), by 2018, the healthcare sector will surpass computing and electronics to become the largest R&D spending industry globally. Since e-Health subject has been one of the most important trends of research world, in recent years, so researchers have especially concentrated on this subject.

8. Statistical Results in Sub-domains of Data Stream

Studying and reviewing papers about this domain show that in the mentioned above publications during two recent years, data stream processing sub-domain with approximate statistic of %62 has covered a huge volume of works

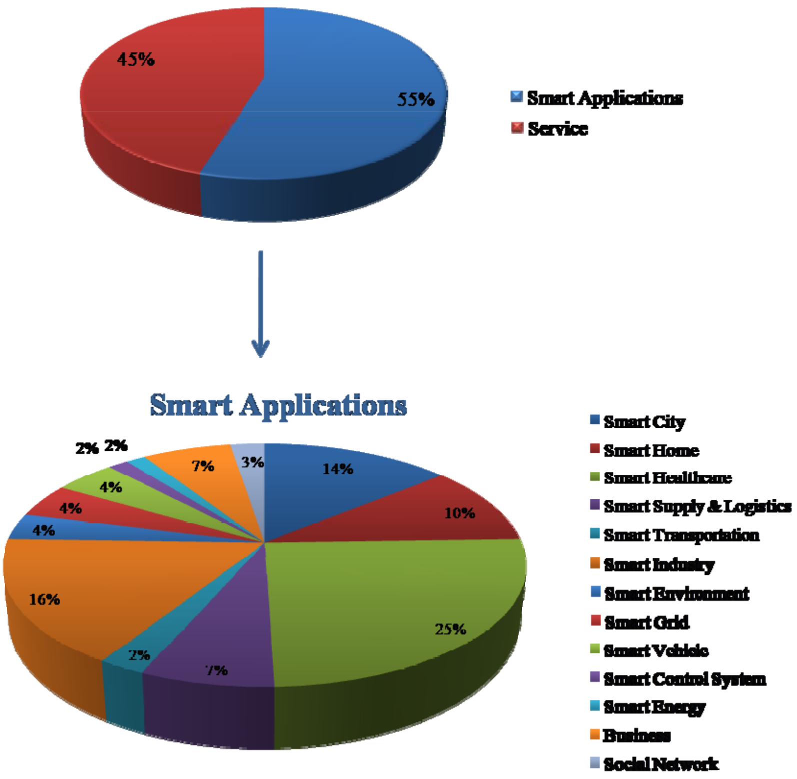

Fig. 10. Statistical Results of Software Services Sub-domains &Smart Applications Sub-subdomains

related to this domain. An important reason for this result may be that data stream processing is a basic step for complex event processing (CEP) process and of course this type of processing as a essential step in IoT big data information value chain is more common in practice. Statistical analysis results have been shown in Fig. 11.

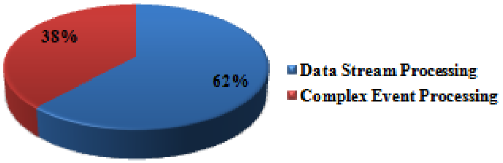

Fig. 11. Statistical Results of Data Stream Sub-domains

9. Statistical Results in Sub-domains of Infrastructure/Hardware

As it is mentioned in previous sections, all hardware equipment used in IoT network has been discussed in the infrastructure domain. According to what has shown in the upper section of the Fig. 12, all conducted studies on IoT infrastructure indicate that the major research works in this domain (about %90), have studied these equipment from the device type point of view. This is while %66 of these all papers related to processing and storage device sub-domains (%33 belongs to each of them similarly). Maybe can be said for why these facts and figures that since resource constrained devices are one of the most challenging topic in terms of processing and storage limitations, thus these types of IoT devices which focus on this two functionality have maximum number of papers. On other hand, among these papers, the minimum amount of research that is only %5, belongs to security devices like IDS and firewall (lower section of Fig. 12). It is to be mentioned that, based on the Fig. 3 which shows research works conducted on the IoT main domains, it is observed trust management with %13 of papers is in the third

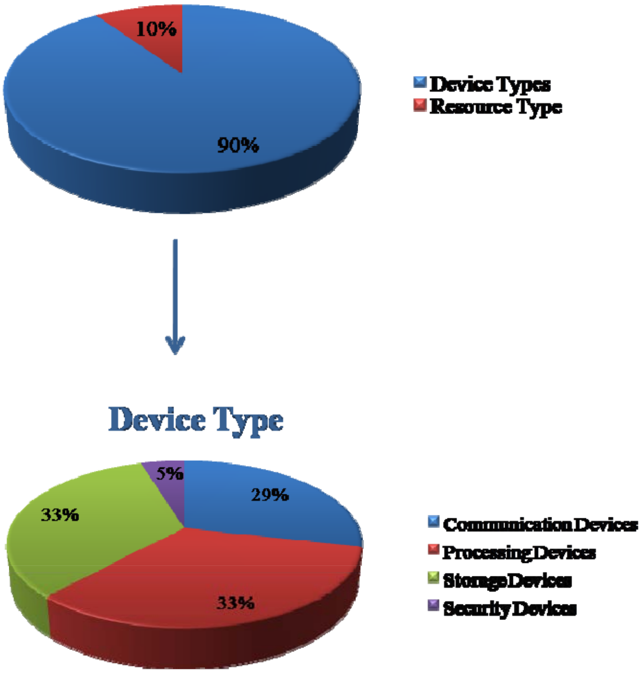

Fig. 12. Statistical Results of Infrastructure/Hardware Sub-domains & Device Type Sub-subdomains

rank after communication. Therefore, since trust management domain has been one of the most applied researches area in recent two years, so the statistical difference between the percentage of conducted works in trust management domain, and security hardware equipment, based on what was said about global R&D trend in above, may describe this reality that the mentioned journals researchers during the past two years tend to investigate software security challenges and issues in IoT rather than to study security equipment issues of this network.

IV. CONCLUSION

Internet of things has been designed as a network of interconnected things/devices, in which devices have independent processing and communication capabilities as well as different storage capacity. In recent years, IoT has significantly developed, and also, it has applied different technologies such as WSN, RFID, and Cloud. Recently, concepts like fog computing and SDN, have been introduced that support M2M communications alongside with related standards and protocols. It must be also mentioned that IoT has wide applications especially in industry and e-health which aims to improve life in human societies. Thus IoT is as the next generation of the network paradigm and service infrastructure, which is evolving and is a trend of future internet.

In this paper, have been investigated and reported the current trends of IoT researches based on papers which have been published in the most famous scientific publications in 2015 & 2016. For this purpose, a top-down approach has been proposed to classify IoT concepts, in research domains and sub-domains structure so that all IoT area concepts have been classified into nine main categories. Then each of these domains has been categorized into some sub-domains based on related concepts. In this regard, some articles related to the sub-domains have been shown in table format. Finally, statistical results of classification have been presented which have obtained from the analysis of reviewed articles. Results show technology and software services domains each one with %19, communication with %14, and trust management with %13 respectively allocate the major portion of studies. Moreover, a detailed analysis of these results indicates main subject of the researches in mentioned domains. In terms of technology issue can be said, WSN as an enabling technology and cloud computing as a supportive technology (%72 and %46 respectively) have attracted the attention of many researchers in comparison with other similar technologies. Also, in software services domain, studies have been concentrated on smart applications including smart healthcare (with the highest percentage), smart industry and smart city. In communication domain, can be concluded that M2M communication and protocols are the most important sub-domains. Also, security in trust management with 68% is more applicable sub-domain in compared to others. Presented results can be a roadmap and an applicable viewpoint for the researchers of IoT area.

REFERENCES

1. Airehrour, D., Gutierrez, J. and Ray, S.K., 2016. Secure routing for internet of things: A survey. Journal of Network and Computer Applications, 66, pp. 198-213.
2. Rajandekar, A. and Sikdar, B., 2015. A Survey of MAC Layer Issues and Protocols for Machine-to-Machine Communications. IEEE Internet of Things Journal, 2(2), pp. 175-186.
3. 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), pp. 585-598.
4. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J. and Leung, K., 2013. A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities, IEEE Wireless Communications, 20(6), pp. 91-98.
5. Di Marco, P., Athanasiou, G., Mekikis, P.-V. and Fischione, C., 2016. MAC-aware routing metrics for the internet of things. Computer Communications, 74, pp. 77-86.
6. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M., 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), pp. 2347-2376.
7. Bandyopadhyay, S., Sengupta, M., Maiti, S. and Dutta, S., 2011. Role of middleware for internet of things: A study, International Journal of Computer Science and Engineering Survey (IJCSES), 2(3), pp. 94-105.
8. Fasolo, E., Rossi, M., Widmer, J. and Zorzi, M., 2007. In-network aggregation techniques for wireless sensor networks: a survey. IEEE wireless communication, 14(2), pp. 70-87.
9. Jin, Y., Gormus, S., Kulkarni, P. and Sooriyabandara, M., 2016. Content centric routing in IoT networks and its integration in RPL. Computer Communications, 89-90, pp. 87-104.
10. Kamalinejad, P., Mahapatra, C., Sheng, Z., Mirabbasi, S., Leung, V.C.M. and Guan, Y.L., 2015. Wireless Energy Harvesting for the Internet of Things. IEEE Communications Magazine, 53(6), pp. 102-108.
11. Yan, Z., Zhang, P. and Vasilakos, A.V., 2014. A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, pp. 120-134.
12. Anzelmo, E., Bassi, A., Caprio, D. and et al., 2011, October. Discussion Paper on the Internet of Things. In 1st Berlin Symposium on Internet and Society: Exploring the Digital Future.
13. Atzori, L., Iera, A. and Morabito, G., 2010. The Internet of Things: A survey. Computer Networks, 54(15), pp. 2787-2805.
14. Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): a vision, architectural elements, and future directions. Future Generation

Computer Systems, 29(7), pp. 1645-1660.

15. Razzaque, M.A., Milojevic-Jevric, M., Palade, A. and Clarke, S., 2016. Middleware for Internet of Things: A Survey. IEEE Internet of Things Journal, 3(1), pp. 70-95.

16. Domingo, M.C., 2012. An overview of the Internet of Things for people with disabilities. Journal of Network and Computer Applications, 35(2), pp. 584-596.

17. Jia, X., Feng, Q., Fan, T. and Lei, Q., 2012, May. RFID technology and its applications in Internet of Things (IoT). In Consumer Electronics, Communications and Networks, 2012, (CECNet). 2nd International Conference on (pp. 1282-1285). IEEE.

18. Liu, C.H., Yang, B. and Liu, T., 2014. Efficient naming, addressing and profile services in Internet-of-Things sensory environments. Ad Hoc Networks, 18, pp. 85-101.

19. Holler, J., Tsiatsis, V., Mulligan, C. and et al., 2014. From Machine-to-Machine to the Internet of Things : Introduction to a new Age of Intelligence. AP Publisher: Academic Press is an imprint of Elsevier.

20. Distefano, S., Merlino, G. and Puliafito, A., 2015. A utility paradigm for IoT: The sensing Cloud. Pervasive and Mobile Computing, 20, pp. 127-144.

21. Li, S., Xu, L.D. and Zhao, S., 2015. The internet of things: a survey. Information Systems Frontiers, 17(2), pp. 243-259.

22. Buyya, R. and Dastjerdi, A.V., 2016. Internet of Things, Principles and Paradigm. 1st Edition, Elsevier Press.

23. Jianguo, X., Gang, X. and Mengmeng, Y., 2013, June. Monitoring system design and implementation based on the Internet of Things. In Digital Manufacturing and Automation (ICDMA). 2013. Fourth International Conference on (pp.801-804). IEEE.

24. Kanagasundaram, R., Majumdar, S., Zaman, M., Srivastava, P. and Goel, N., 2012, July. Exposing resources as Web services: a performance oriented approach. In symposium of performance evaluation of computer and telecommunication systems (SPECTS), 2012. International symposium on. IEEE.

25. Rong, Y., Li, B. and HU, Y., 2016. An Experimental Study for Intelligent Logistics: A Middleware Approach. Chinese Journal of Electronics, 25(3), pp. 561-569.

26. Antoni, A., Marjanovi, M., Pripuzic, K. and Zarko, I.P., 2016. A mobile crowd sensing ecosystem enabled by CUPUS-Cloud-based publish-subscribe middleware for the Internet of Things. Future Generation Computer Systems, 56, pp. 607-622.

27. Balakrishnan, S.M. and Sangaiah, A.K., 2017. MIFIM-Middleware solution for service centric anomaly in future internet models. Future Generation Computer Systems, 74, pp. 349-365.

28. Jiang, H., Zhao, S., Zhang, Y. and Chen, Y., 2012. The cooperative effect between technology standardization and industrial technology innovation based on Newtonian mechanics. Information Technology and Management, 13(4), pp. 251-262.

29. Teklemariam, G.K., Hoebeke, J., Moerman, I. and Demeester, P., 2013. Facilitating the creation of IoT applications through conditional observations in CoAP. EURASIP Journal on Wireless Communications and Networking.

30. Castellani, A.P., Bui, N., Casari, P. and et al., 2010. Architecture and protocols for the internet of things: a case study. In pervasive computing and communications workshops (PERCOM workshops). Eighth international conference on (pp. 678-683), IEEE.

31. Lee, I-G. and Kim, M., 2016. Interference-aware self-optimizing Wi-Fi for high efficiency internet of things in dense networks. Computer Communications, 89-90, pp. 60-74.

32. Collotta, M. and Pau, G., 2015. Bluetooth for Internet of Things: A fuzzy approach to improve power management in smart homes. Computers and Electrical Engineering, 44, pp. 137-152.

33. Buratti, C., Stajkic, A., Gardasevic, G. & et al. (2015). Testing Protocols for the Internet of Things on the EuWIn Platform. IEEE Internet of Things Journal.

34. Akgün, M. and Çaglayan, M.U., 2015. Providing destructive privacy and scalability in RFID systems using PUFs. Ad Hoc Networks, 32, pp. 32-42.

35. He, D., Kumar, N. and Lee, J-H., 2015. Secure pseudonym-based near field communication protocol for the consumer internet of things. IEEE Transactions on Consumer Electronics, 61(1), pp. 56-62.

36. Ghaleb, S.M., Subramaniam, S. , Zukarnain, Z.A. and Muhammed, A., 2016. Mobility management for IoT: a survey. EURASIP Journal on Wireless Communications and Networking.

37. Sheng, Z., Wang, H., Yin, C., Hu, X., Yang, S. and Leung, V.C.M., 2015. Lightweight Management of Resource-Constrained Sensor Devices in Internet of Things. IEEE Internet of Things Journal, 2(5), pp. 402-411.

38. Betzler, A., Gomez, C., Demirkol, I. and Paradells, J., 2015. CoCoA+: An advanced congestion control mechanism for CoAP. Ad Hoc Networks, 33, pp. 126-139.

39. Rimal, B.P., Choi, E. and Lumb, I., 2009, August. A taxonomy and survey of cloud computing systems. In INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on (pp. 44-51). IEEE.

40. Mehmood, Y., Görg, C., Muehleisen, M. and Timm-Giel, A., 2015. Mobile M2M communication architectures, upcoming challenges, applications, and future directions. EURASIP Journal on Wireless Communications and Networking.

41. Kovatsch, M., Lanter, M. and Shelby, Z., 2014. Californium: scalable cloud services for the internet of things with CoAP. In the Internet of Things (IoT 2014). fourth international conference on.

42. Amadeo, M., Briante, O., Campolo, C., Molinaro, A. and Ruggeri, G., 2016. Information-centric networking for M2M communications: Design and deployment. Computer Communications, 89-90, pp. 105 –116.

43. Aijaz, A. and Aghvami, H., 2015. Cognitive Machine-

to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective. IEEE Internet of Things Journal, 2(2), pp. 103-112.

44. Bouaziz, M., and Rachedi, A., 2015. A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology. Computer Communications, 74, pp. 3-15.

45. Misic, J., Shafi, S. and Misic, V.B., 2006. Performance limitations of the MAC layer in 802.15.4 low rate WPAN. Computer Communications, 29(13-14), pp. 2534–2541.

46. Park, P., Marco, P.D., Fischione, C. and Johansson, K.H., 2013. Modeling and Optimization of the IEEE 802.15.4 Protocol for Reliable and Timely Communications. IEEE Transactions on Parallel and Distributed Systems, 24(3), pp. 550-564.

47. Ergen, S.C., Marco, P.D. and Fischione, C., 2009, December. MAC Protocol engine for sensor networks. In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE.

48. Hakak, S., Latif, S.A., Gilkar, G. and Alam, M.K., 2014, May. Performance analysis of DYMO and DSR protocols under variation of DSSS rate. In Informatics, Electronics & Vision (ICIEV), 2014. 3rd International Conference on. IEEE.

49. Karlsson, J., Dooley, L.S. and Pulkkis, G., 2012. Routing security in mobile ad-hoc networks. Issues in Informing Science and Information Technology, 9, pp. 369-383.

50. Qiu, T., Lv, Y., Xia, F. and et al., 2016. ERGID: An efficient routing protocol for emergency response Internet of Things. Journal of Network and Computer Applications, 72, pp. 104-112.

51. Sicari, S., Rizzardi, A., Grieco, L.A., and Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. Computer Network, 76, pp. 146-164.

52. Turkanovic, M., Brumen, B. and Hölbl, M., 2014. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks, 20, pp. 96-112.

53. Farash, M.S., Turkanović, M., Kumari, S. and Hölbl, M., 2015. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks, 36, pp. 152-176.

54. Amin, R., Islam, SK. H., Biswas, G.P. and et al., 2016. Design of anonymity preserving three-factor authenticated key exchange protocol for wireless sensor network. Computer Networks, 101, pp. 42-62.

55. Li, J., Wen, M. and Zhang, T., 2016. Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A Networks. IEEE Internet of Things Journal, 3(3), pp. 408-417.

56. Li, F., Han, Y. and Jin, C., 2016. Practical access control for sensor networks in the context of the Internet of Things. Computer Communications, 89-90, pp. 154-164.

57. Lee, J., Seo, J.W., Ko, H. and Kim, H., 2017. TARD: Temporary Access Rights Delegation for guest network devices. Journal of Computer and System Sciences, 86, pp. 59-69.

58. Rizzardi, A., Sicari, S., Miorandi, D. and Coen-Porisini, A., 2016. AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things. Information Systems, 62, pp. 29-41.

59. Chatzigiannakis, I., Vitaletti, A. and Pyrgelis, A., 2016. A privacy-preserving smart parking system using an IoT elliptic curve based security platform. Computer Communications, 89-90, pp.165-177.

60. Avoine, G., Bingol, M., Carpent, X. and Yalcin, S., 2013. Privacy-friendly authentication in RFID systems: on sublinear protocols based on symmetric-key cryptography. IEEE Transactions on Mobile Computing, 12(10), pp. 2037–2049.

61. Jacobsson, A., Boldt, M. and Carlsson, B., 2016. A risk analysis of a smart home automation system. Future Generation Computer Systems, 56, pp. 719-733.

62. Liu, A., Zhang, Q., Li, Z. and et al., 2017. A green and reliable communication modeling for industrial internet of things. Computers and Electrical Engineering, 58, pp. 364-381.

63. Ahmad, M. and Jose, S., 2015, May. Designing for the Internet of Things: A Paradigm Shift in Reliability. In Electronic Components and Technology Conference (ECTC), 2015. 65th International Conference on (pp. 1758-1766). IEEE.

64. Park, J.H., 2016. All-terminal reliability analysis of wireless networks of redundant radio modules. IEEE Internet of Things Journal, 3(2), pp. 219-230.

65. Nessa, A. and Kadoch, M., 2016, Joint Network Channel Fountain Schemes for Machine Type Communications over LTE-Advanced. IEEE Internet of Things Journal, 3(3), pp. 418- 427.

66. Dimitriou, T., 2016. Key Evolving RFID Systems: Forward/Backward Privacy and Ownership Transfer of RFID tags. Ad Hoc Networks, 37(2), pp. 195–208.

67. Rawat, P., Singh, K.D., Chaouchi, H. and Bonnin, J.M., 2014. Wireless sensor networks: a survey on recent developments and potential synergies. The Journal of Supercomputing, 68(1), pp. 1-48.

68. Lee, B. and Kim, S-J., 2015. Energy-efficient sensor device personalization scheme for the internet of things and wireless sensor networks. IEICE Transactions on Communications Journal, E98.B(1), pp. 231-241.

69. Sheng, Z., Mahapatra, C., Zhu., C. and Leung, V.C.M., 2015. Recent advances in industrial wireless sensor networks toward efficient management in IoT. IEEE Access Journal, 3, pp. 622-637.

70. Porambage, P., Braeken, A. and Schmitt, C., 2015. Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications. IEEE Access Journal, 3, pp. 1503-1511.

71. Díaz, M., Martín, C. and Rubio, B., 2016. State-

of-the-art, challenges, and open issues in the integration of Internet of Things and Cloud Computing. Journal of Network and Computer Applications, 67, pp. 99-117.

72. Xu, Y. and Hela, S., 2016. Scalable Cloud-Sensor Architecture for the Internet of Things. IEEE Internet of Things Journal, l3(63), pp. 285 - 298.

73. Chen, C., Bose, R. and Helal, A., 2009. Atlas: An Open Model for Automatic Integration and Teleprogramming of Smart Objects. In Design and Integration Principles for Smart Objects, 2009. DIPSO'09. 3rd International Workshop on.

74. Luo, S. and Ren, B., 2016. The Monitoring and Managing Application of Cloud Computing Based on Internet of Things. Computer Methods and Programs in Biomedicine, 130(C), pp. 154-161.

75. Škraba, A., Stojanovic, R., Zupan, A., Koložvari, A. and Kofjač, D., 2015. Speech-controlled cloud-based wheelchair platform for disabled persons. Microprocessors and Microsystems, 39(8), pp. 819-828.

76. Persson, P. and Angelsmark, O., 2015. Calvin – Merging Cloud and IoT. Procedia Computer Science, 52, pp. 210-217.

77. Tanenbaum, A.S, 1994. Distributed operating systems, first edition, Pearson.

78. Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D. and Ohlman, B., 2012. A survey of information-centric networking. IEEE Communications Magazine, 50(7), pp. 26-36.

79. Baccelli, E., Mehlis, C., Hahm, O. and Schmidt, T.C., 2014. Information Centric Networking in the IoT: Experiments with NDN in the Wild. In Information-Centric Networking, 2014. ACM-ICN '14. 1st Conference on. (pp. 77-86). ACM.

80. Xylomenos, G., Ververidis, C.N., Siris, V.A., and et al., 2014. A survey of information-centric networking research. IEEE Communications Surveys & Tutorials, 16(2), pp. 1024-1049.

81. Jin, Y., Kulkarni, P., Gormus, S. and Sooriyabandara, M., 2012, October. Content centric and load balancing aware dynamic data aggregation in multi-hop wireless networks. In Wireless and Mobile Computing, Networking and Communications (WiMob), 2012. 8th International Conference on (pp. 179-186). IEEE.

82. Kim, H., Benson, T., Akella, A. and Feamster, N., 2011, November. The evolution of network configuration: a tale of two campuses. In Internet measurement conference, 2011. IMC'11. SIGCOMM conference on (pp. 499-514). ACM.

83. https://www935.ibm.com/services/au/gts/pdf/200249.pdf, last accessed on September 2016.

84. Xia, W., Wen, Y., Foh, C.H., Niyato, D. and Xie, H., 2015. A Survey on Software-Defined Networking. IEEE Communications Surveys & Tutorials, 17(1), pp. 27-51.

85. https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf. last accessed on September 2016.

86. Jararweh, Y., Al-Ayyoub, M., Darabseh, A. and Rindos, A., 2015. SDIoT: a software defined based internet of things framework. Journal of Ambient Intelligence and Humanized Computing, 1(4), pp. 453-461.

87. Hakiri, A., Berthou, P. and Gokhale, A., 2015. Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications. IEEE Communications Magazine, 53(9).

88. Liu, J., Li, Y. and Chen, M., 2015. Software-defined internet of things for smart urban sensing. IEEE Communications Magazine, 53(9).

89. Aazam, M. and Huh, E.N., 2014, August. Fog Computing and Smart Gateway Based Communication for Cloud of Things. In Future Internet of Things and Cloud (FiCloud), 2014. International Conference on (pp. 464-470). IEEE.

90. Sehgal, V.K., Patrick, A., Soni, A. and Rajput, L., 2015. Smart human security framework using internet of things, Cloud and fog computing. Part of the Advances in Intelligent Systems and Computing book series, Springer Publisher.

91. Zhou, Z., Zhao, D., Xu, X., Du, C. and Sun, H., 2015. Periodic Query Optimization Leveraging Popularity-Based Caching in Wireless Sensor Networks for Industrial IoT Applications. Mobile Networks and Applications Journal, 20(2), pp. 124-136.

92. Zhai, C., Zou, Z., Chen, Q. and et al., 2016. Delay-Aware and Reliability-Aware Contention-Free MF-TDMA Protocol for automated RFID monitoring in industrial IoT. Journal of Industrial Information Integration, 3, pp. 8-19.

93. Catarinucci, L., Donno, D.D., Mainetti, L. and et al., 2015. An IoT-Aware Architecture for Smart Healthcare Systems. IEEE Internet of Things Journal, 2(6), pp. 515 - 526.

94. Suarez, J., Quevedo, J., Vidal, I. and et al., 2016. A secure IoT management architecture based on Information-Centric Networking. Journal of Network and Computer Applications, 63, pp. 190-204.

95. Quevedo, J., Antunes, M., Corujo, D., Gomes, D. and Aguiar, R.L., 2016. On the application of contextual IoT service discovery in Information Centric Networks. Computer Communications, 89-90, pp.117 –127.

96. Gu, Z. and Zhao, Q., 2012. A state-of-the-art survey on real-time issues in embedded systems virtualization. Journal of Software Engineering and Applications, 5, pp. 277-290.

97. Morabito, R., 2017. Virtualization on Internet of Things Edge Devices With Container Technologies: A Performance Evaluation. IEEE Access. 5, pp. 8835 – 8850.

98. Ali, Z.H., Ali, H.A. and Badawy, M.M., 2017. A New Proposed the Internet of Things (IoT) Virtualization Framework Based on Sensor-as-a-Service Concept. Wireless Personal Communications, 97(1), pp. 1419-1443.

99. Liu, W., Nishio, T., Shinkuma, R. and Takahashi, T., 2014. Adaptive resource discovery in mobile cloud computing. Computer Communications, 50, pp. 119-129.

100. Djamaa, B., Yachir, A. and Richardson, M., 2017.

Hybrid CoAP-based resource discovery for the Internet of Things. Journal of Ambient Intell Human Comput, 8(3), pp. 357-372.

101. Nishio, T., Shinkuma, R., Takahashi, T. and Mandayam, N.B., 2013, July. Service-oriented heterogeneous resource sharing for optimizing service latency in mobile cloud. In Mobile cloud computing & networking, 2013. MobileCloud '13. first international workshop on (pp. 19-26), ACM.

102. Maia, A.M., Vieira, D., de Castro, M.F. and Ghamri-Doudane, Y., 2016. A fair QoS-aware dynamic LTE scheduler for machine-to-machine communication. Computer Communications, 89-90, pp. 75-86.

103. Kim, T-Y. and Kim, E-J., 2016. Uplink scheduling of MU-MIMO gateway for massive data acquisition in Internet of things. The Journal of Supercomputing, pp. 1-15.

104. Narman, H.S., Hossain, M.S., Atiquzzaman, M. and Shen, H., 2017. Scheduling internet of things applications in cloud computing. Annals of Telecommunications, 72(1-2), pp. 79-93.

105. Abdullah, S. and Yang, K., 2014. An Energy Efficient Message Scheduling Algorithm Considering Node Failure in IoT Environment. Wireless Personal Communications, 79(3), pp. 1815-1835.

106. Chun, B-G., Ihm, S., Maniatis, P., Niak, M. and Patti, A., 2011, April. Clonecloud: elastic execution between mobile device and cloud. In Computer systems, 2011. EuroSys'11. sixth conference on (pp. 301-314). ACM.

107. Kosta, S., Aucinas, A., Hui, P., Mortier, R. and Zhang, X., 2012, March. Thinkair: dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In INFOCOM, 2012. (pp. 945-953). IEEE.

108. Gordon, M.S., Jamshidi, D.A., Mahlke, S. and Mao, Z.M., 2012, October. COMET: code offload by migrating execution transparently. In Operating Systems Design and Implementation, 2012. OSDI'12. 10th USENIX conference on (pp. 93-106), ACM.

109. Kim, S., 2015. Nested game-based computation offloading scheme for Mobile Cloud IoT systems. EURASIP Journal on Wireless Communications and Networking, pp. 229-239.

110. Flores, H., Hui, P., Tarkoma, S. and et al., 2015. Mobile Code Offloading: From Concept to Practice and Beyond. IEEE Communications Magazine, 53(3), pp. 80-88.

111. Park, Y. and Kim, S., 2015. Game-based data offloading scheme forIoT system traffic congestion problems. EURASIP Journal on Wireless Communications and Networking, pp. 192-201.

112. Li, L., Li. S. and Zhao, S., 2014. QoS-Aware Scheduling of Services-Oriented Internet of Things. IEEE Transactions on Industrial Informatics, 10(2).

113. Pradilla, J., Palau, C. and Esteve, M., 2015. SOSLite: Lightweight Sensor Observation Service (SOS). IEEE Latin America Transactions, 13(12), pp. 3758-3764.

114. Yerra, R., Kiran , M.P.R.S. and Pachamuthu, R., 2015. Reliability and delay analysis of slotted anycast multi-hop wireless networks targeting dense traffic iot applications. IEEE Communications Letters Journal, 19(5), pp. 727-730.

115. Poslad, S., 2015. A Semantic IoT Early Warning System for Natural Environment Crisis Management. IEEE Transactions on Emerging Topics in Computing, 3(2), pp. 246-257.

116. Fang, S., Xu, L., Zhu, Y. and et al., 2015. An integrated information system for snowmelt flood early-warning based on internet of things. Information Systems Frontiers, 17(2), pp. 321-335.

117. Mayer, R., Koldehofe, B. and Rothemel, K., 2015. Predictable Low-Latency Event Detection With Parallel Complex Event Processing. IEEE Internet of Things Journal, 2(4), pp. 274-286.

118. Yang, P., 2015. PRLS-INVES: A General Experimental Investigation Strategy for High Accuracy and Precision in Passive RFID Location Systems. IEEE Internet of Things Journal, 2(2), pp. 159-167.

119. Vermesan, O. and Friees, P., 2014. Internet of Things - From Research and Innovation to Market Deployment. River Publisher.

120. Smith, I.G., Vermesan, O., Friees, P. and Furness, A., 2012. The Internet of Things 2012 New Horizons. Halifax Publisher, UK.

121. Zhou, L., Sheng, Z., Wei, L. and et al., 2016. Green cell planning and deployment for small cell networks in smart cities. Ad Hoc Network, 43, pp. 30-42.

122. Lolis, L., Bernir, C., Pelissier, M., Dallet, D. and Begueret, J.B., 2010, June. Bandpass Sampling RX System Design Issues and Architecture Comparison for Low Power RF Standards. In Circuits and Systems (ISCAS), 2010. International Symposium on (pp. 3921-3924). IEEE.

123. Hayashi, Y., Yahagi, K., Sato, H., Sato, K. and Muratani, M., 2015, August. "Easy-to-use" RF-solutions for IoT applications. In Radio-Frequency Integration Technology (RFIT), 2015. International Symposium on (pp. 13-15). IEEE.

124. Bousseaud, P., Novakov, E. and Fournier, J.M., 2015, October. A direct RF signal sampling integrated receiver for IoT applications. In Advanced Technologies for Communications (ATC), 2015. International Conference on (pp. 237-242). IEEE.

125. Liu, Y., Ren, K.L., Hofmann, H.F. and Zhang, Q., 2005. Investigation of electrostrictive polymers for energy harvesting. IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, 52(12), pp. 2411-2417.

126. Cengiz, K. and Dag, T., 2015. A review on the recent energy-efficient approaches for the Internet protocol stack. EURASIP Journal on Wireless Communications and Networking, pp. 108-129.

127. Gorlatova, M., Sarik, J., Grebla, G. and et al., 2015. Movers and Shakers: Kinetic Energy Harvesting for the Internet of Things. IEEE Journal on Selected Areas in Communications, 33(8), pp. 1624-1639.

128. Wang, Y., Liu, Y., Wang, C. and et al., 2016. Storage-less and Converter-less Photovoltaic Energy Harvesting with

Maximum Power Point Tracking for Internet of Things. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 35(2), pp. 173-186.

129. Kim, S. and Kim, S., 2016. A multi-criteria approach toward discovering killer IoT application in Korea. Technological Forecasting & Social Change, 102, pp. 143–155.

130. Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M. and Kwak, K-S., 2015. The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 3, pp. 678-708.

131. Luo, X., Liua, J., Zhanga, D. and Chang, X., 2016. A large-scale web QoS prediction scheme for the Industrial Internet of Things based on a kernel machine learning algorithm. Computer Networks, 101, pp. 81-89.

132. Rathore, M.M., Ahmad, A., Paul, A. and Rho, S., 2016. Urban planning and building smart cities based on the Internet of Things using Big Data analytics. Computer Networks, 101, pp. 63-80.

133. Gigli, M. and Koo, S., 2011. Internet of Things: Services and applications categorization. Advances in Internet of Things (AIT), 1(2), pp. 27–31.

134. Xiaojiang, X., Jianli, W. and Mingdong, L., 2010. Services and key technologies of the Internet of Things. ZTE Communication, 8(2), pp. 26-29.

135. Ruckebusch, P., Poorter, E.D., Fortuna, C. and Moerman, I., 2016). GITAR: Generic extension for Internet-of-Things ARchitectures enabling dynamic updates of network and application modules. Ad Hoc Networks, 36(1), pp. 127-151.

136. Barbon, G., Margolis, M., Palumbo, F., Raimond, F. and Weldin, N., 2016. Taking Arduino to the Internet of Things: The ASIP programming model. Computer Communications, 89-90, pp. 128-140.

137. Nastic, S., Truong, H-L. and Dustdar, S., 2015. SDG-Pro: a programming framework for software-defined IoT cloud gateways. Journal of Internet Services and Applications, 6, pp. 21-37.

138. Silva, J.A., Faria, E.R., Barros, R.C. and et al., 2013. Data stream clustering: A survey. ACM Computing Surveys, 46(1).

139. Qin, Y., Sheng, Q.Z., Falkner, N.J.G. and et al., 2016. When things matter: A survey on data-centric internet of things. Journal of Network and Computer Applications, 64, pp. 137-153.

140. Liu, J., Fang, C. and Ansari, N., 2016. Request Dependency Graph: A Model for Web Usage Mining in Large-scale Web of Things. IEEE Internet of Things Journal, 3(4), pp. 598 - 608.

141. Poghosyan, G., Pefkianakis, I., Le Guyadec, P. and Christophides, V., 2016. Mining usage patterns in residential intranet of things. Procedia Computer Science, 83, pp. 988-993.

142. Zhu, T., Dhelim, S., Zhou, Z., Yang, S. and Ning, H., 2017. An architecture for aggregating information from distributed data nodes for industrial internet of things. Computers and Electrical Engineering, 58, pp. 337-349.

143. Mehdiyev, N., Krumeich, J., Enke, D., Werth, D. and Loos, P., 2015. Determination of Rule Patterns in Complex Event Processing Using Machine Learning Techniques. Procedia Computer Science, 61, pp. 395-401.

144. Mostefaoui, A., Noura, H. and Fawaz, Z., 2015. An integrated multimedia data reduction and content confidentiality approach for limited networked devices. Ad Hoc Networks, 32, pp. 81-97.

145. Serdaroglu, K.C. and Baydere, S., 2016. WiSEGATE: Wireless Sensor Network Gateway framework for internet of things. Wireless Networks, 22(5), pp. 1475–1491.

146. Xu, Q., Aung, K.M.M., Zhu, Y. and Yong, K.L., 2016. Building a large-scale object-based active storage platform for data analytics in the internet of things. The Journal of Supercomputing, 72(7), pp. 2796-2814.

147. Jiang, H., Shen, F., Chen, S., Li, K-C. and Jeong, Y-S., 2015. A secure and scalable storage system for aggregate data in IoT, Future Generation Computer Systems, 49, pp. 133-141.

148. Kizza, J.M., 2015. Guide to Computer Network Security. The Computer Communications and Networks book series. London: Springer.

149. Raza, S., Voigt, T. and Wallgren, L., 2013. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8), pp. 2661-2674.

150. Costamagna, G., Kasinathan, P., Khaleel, H., Pastrone, C. and Spirito, M.A., 2013, November. DEMO: An IDS framework for internet of things empowered by 6LoWPAN. In Computer & communications security, 2013. CCS'13. SIGSAC conference on (pp. 1337-1340). ACM.

151. Kubler, S., Främling, K. and Buda, A., 2015. A standardized approach to deal with firewall and mobility policies in the IoT. Pervasive and Mobile Computing, 20, pp. 100-114.

152. Russell, B. and Duren, D.V., 2016. Practical Internet of Things Security. Packt Publishing.