Assessing Trends of Existing Research Contribution Towards Internet-of-Things

Bhagyashree Ambore (Assistant Professor)[1], Dr. Suresh L (Principal and Professor)[2]
Dept of computer science & Engg.
Cambridge Institute of Technology
Bangalore, India

***Abstract*—With the growing demands of system automation, technology integration, and non-human intervention technique, Internet-of-Things (IoT) has evolved as a boon and value-added services over pervasive computing. IoT comprises a highly complex system that integrates ubiquitous computing with low-powered data capturing devices via a gateway. Along with various forms of unimaginable advantages, IoT is also associated with a huge list of ongoing problems. The prime objective of the paper is to gauge the effectiveness of existing works of literature being carried out towards mitigating the issues of IoT. The paper illustrates the most frequently explored research topic and less regularly explored topic in IoT for providing a true picture of existing research trends. The paper also idealizes some of the research gaps that have been extracted after reviewing the existing literature.**

***keywords*—Bandwidth; cloud computing; energy; internet-of-things; security; sensor network**

I. Introduction

The area of network and communication system is in the faster process of evolution and has witnessed tremendous advancements in its technologies in most recent years. IoTor commonly known as IoT is one of such technological advancement, which has been born by the amalgamation of network and various forms of devices to capture data [1]. Technically speaking, IoT is a sophisticated network of low-powered embedded devices with the large connectivity of the network. Fig.1 shows one of the typical schemas of IoT. The schema shows four different top-down layers. The bottom layer is the sensors, which is responsible for capturing the raw information from the environment, which is connected to the IoT devices in the next upper layer. The data is finally aggregated from IoT devices and forwarded to the wired or wireless terminal, which uses gateway services to process the data to the top layer. The top layer is the data center which offers various forms of cloud-based services over the internet to the users [2]. Hence, IoT primarily assists the sensors to capture the information and forward it to the user using cloud services [3]. However, IoT is not that easy as it seems like. The term *thing* in IoT is not necessarily sensors; it could be any form of a low-powered device. However, it should be understood that IoT is a very futuristic technology that enables fair communication between two different kinds of machines with the incorporation of the higher degree of system automation and thereby avoid intervention from human [4].

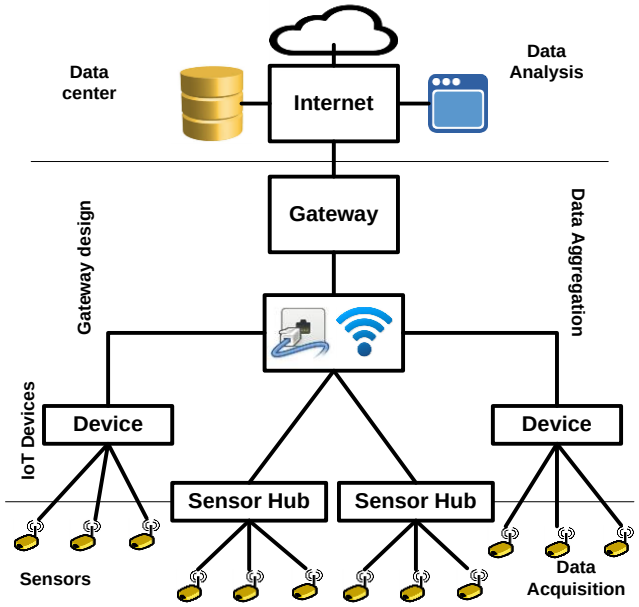

Fig. 1. IoT Typical Schema.

Usage of IoT will lead better task automation, better return on investment, however, it is also associated with issues, e.g., i) IoT doesn't provide any standardization for tagging, ii) IoT has the most challenging complexity in its system design (a minor fault in the system will result in entire malfunction), iii) privacy and security standard could be easily compromised, iv) device compatibility is another severe issues in IoT, and v) lack of human intervention. Although IoT is a very novel technology, it is also one of the burning topics among the researchers. Hence, this paper intends to understand the existing research work towards IoT and targets to understand the effectiveness of the existing research contribution. The prime contribution of this paper is to identify the scale of the effectiveness of existing research work. Section II discusses the important information pertaining to IoT very briefly with respect to its essential characteristics and existing frameworks. The standard IoT architectures are discussed in Section III. Section IV discusses existing survey work in IoT followed by existing research trends in Section V. Section VI addresses the research gap identified from critical analysis of existing research trend in IoT. Finally, Section VII concludes the paper with the idea of future work.

II. ESSENTIALS OF IOT

IoT is one of the upcoming trends of technological advancement, which has started created news right from now. IoT is the connectivity of various forms of electronic devices, which are terms as *the thing* with a unique identification. This electronic device senses certain physical attribute, process them using various software and transmits the information using heterogeneous or homogeneous networking protocols [5]. The prime purpose of IoT is not only to sense but also to perform certain controlling mechanism over the things remotely. IoT essentially creates a bridge between computing and the physical world. The application areas of IoT involves smart cities, home automation, smart manufacturing, health care, wearables, automotive, transportation, etc. [6]. Various technologies assist in enabling the operationality in IoT applications. RFID (Radio Frequency Identification) is one of the best enabling technology in IoT that connects various objects with internet [7]. Near-Field Communication is another enabling technology of IoT applications [8]. The existing system also uses cost-effective communication schemes, e.g., QR codes, optical tags, etc. [9]. Bluetooth and sensors are the most recent evolution of the existing enabling technologies of IoT. Along with novelty, cut-edge features, there are associated challenges with IoT.

A. Characteristics of IoT

The application that uses IoT basically encounters various challenging scenarios (discussed in the next sub-section). Owing to the novelty in the technology, it is essential to understand the most critical characteristics of IoT, which are as discussed briefly as follows,

- *Usage of Intelligence:* The fundamental design principle of IoT is based on autonomous control and Ambient Intelligence. The future applications of IoT are expected to be highly self-organization with the interoperable virtual object, where circumstances, context, and environments play a significant role.
- *Seamless Connectivity:* The different embedded devices that are connected by IoT are required to possess undisturbed accessibility.
- *Potential Sensing Capability:* Sensing a particular physical world attribute is one of the essential features of IoT. The sensed data are considered as input for the majority of IoT applications.
- *Massive Number of things:* The upcoming IoT comprises of connectivity of more than millions of sensing and controlling devices.
- *Energy Efficiency*: Incorporations of the higher degree of energy conservation is another significant feature of IoT as the majority of the IoT applications operate on adverse environmental condition that calls for unattended operation.
- *Secure Network:* Owing to the inclusion of multiple forms of networking and data processing protocols, potential security features become one mandatory target in IoT.

B. IoT Frameworks:

The framework involved in IoT assists in formulating the interaction between the devices (or *things*) and permit for better-sophisticated supportability of distributed computing. Some of the well-known structures of IoT are:

- *Jasper:* It is one of the frequently used frameworks that provide an operational platform of rending the communication system among the devices. It is used on automotive applications in IoT utilizing the cloud. The framework assists car manufacturing organization to surveil the defects, insignificant correctness features in automotive. It also checks for successful security incorporations in transportation. A reputed organization, e.g., GE aviation, Coca-Cola, Audi, etc. already use Jasper for offering better services in their products [9].
- *Arrayant:* It is a form of the framework that assists in connecting the services or products with the manufacturer using the internet. It is delivered along with the framework with respect to SaaS. It also consists of a managed cloud for assisting device connectivity, software toolkits for developing web applications, and software library to connect the device with service on the internet [10].
- *AggreGate:* It is a computational framework that is used for managing various forms of embedded devices with multiple forms of data. It is mainly used in the manufacturing organization. Along with controlling various devices, it also offers automation, network management, monitoring attendance, managing data center, managing fleet, controlling sensor network, management of the mobile device, and controlling physical access [11].
- *Xively:* It is another frequently used framework for IoT that has the potential to connect any devices for carrying out communication with other particular devices using the internet. It also offers a cloud-based service (e.g., PaaS) for IoT-based services, e.g., data services, security engine, directory services, etc. Xively can be used with open source libraries with hardware and various APIs [12].
- *Carriots:* It is a software framework with the uniqueness of application hosting and features of PaaS for IoT applications. The framework is known for its capability of collecting valuable data from the devices and then processes it to make it suitable for a specific IT infrastructure. It is characterized by custom alerts, device management, SDK applications, API management, data export, etc. [13].
- *Everything:* It is another typical IoT framework that can access data and control any for any physical devices. It can perform integration of tags, SDK, and controllers. The administration, as well as analytics, also characterizes it. This framework is used for real-time data management, managing various product connections, integration with multiple forms of

hardware devices connected with internet, Cloud PaaS, Analytics and Administration, and security (or access) control [14].

III. IOT ARCHITECTURE

The architecture followed by an organization to undertake IoT solution for their business to run is termed as *Reference Architecture*. It is a customizable architecture that defines the essential characteristics of required performance, critical functional requirements, execution, and security incorporation with industry-based standards [15]. Fig.2 highlights existing reference architecture of IoT, which is the base of all the well-defined architectures. One of the essential blocks of this architecture is called as *Reference Model*, which is again build up by three components, i.e., business vision, IoT Reference Model, and IoT Reference Architecture. The usage of IoT Architectural Reference model is shown in Fig.3, where it can be seen that it acts as enabling IoT architectural schema in system design of IoT-based applications. The system design, however, takes the input from the use cases and requirements which depend on the business concerns. The system design is also enabled by significant engineering strategies of usage of multiple technologies to make it operational. All these processes finally lead to the generation of concrete architecture for a specific, concrete architecture of IoT. The business vision component comprises all the essential requirements of business that finally acts as the industry standard to control the architecture. The component of *the Reference Model* furnishes higher abstraction level for supporting a comprehensive understanding of IoT domain. The component of the reference architecture is considered as the building block of all the major architectures of IoT. Various existing architectures, concerns of business as well as solutions are considered as input for existing IoT Architectural Reference Model via *SOTA* (Software updates Over The Air) using cloud services. After performing extrapolation, all these preliminary requirements transform itself into a single and joint requirement for reference architecture of IoT. Hence, the most critical part of the IoT architecture is to perform a unified understanding of multiple domains of IoT in terms of modeling.

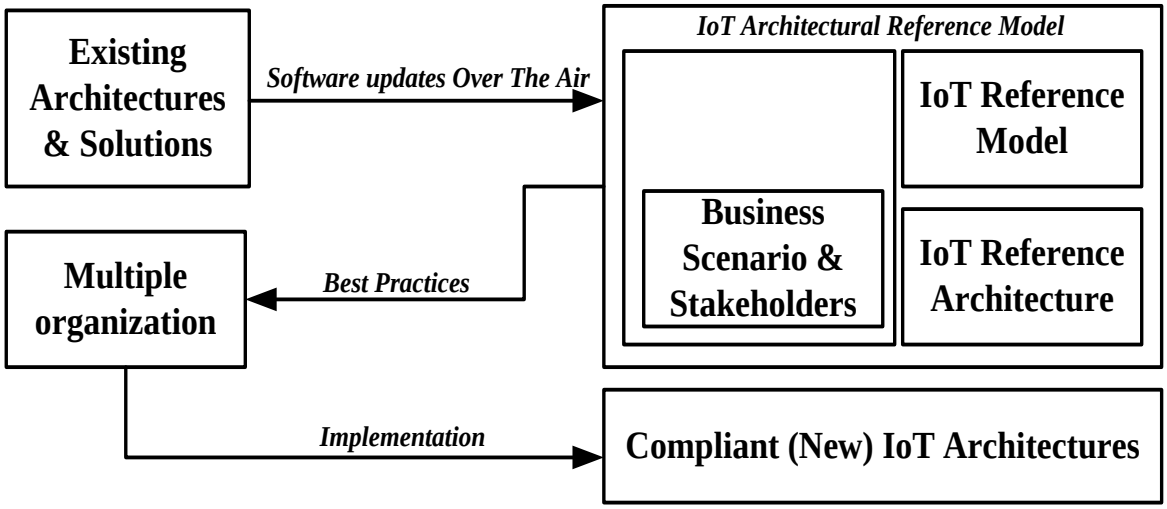

Fig. 2. Existing Reference Architecture of IoT [15].

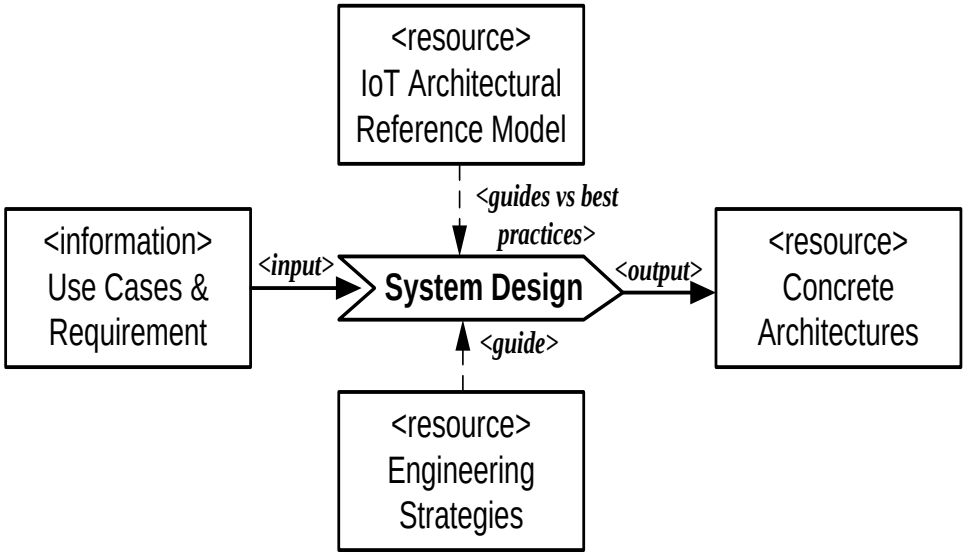

Fig. 3. Formation of Concrete Architecture [15].

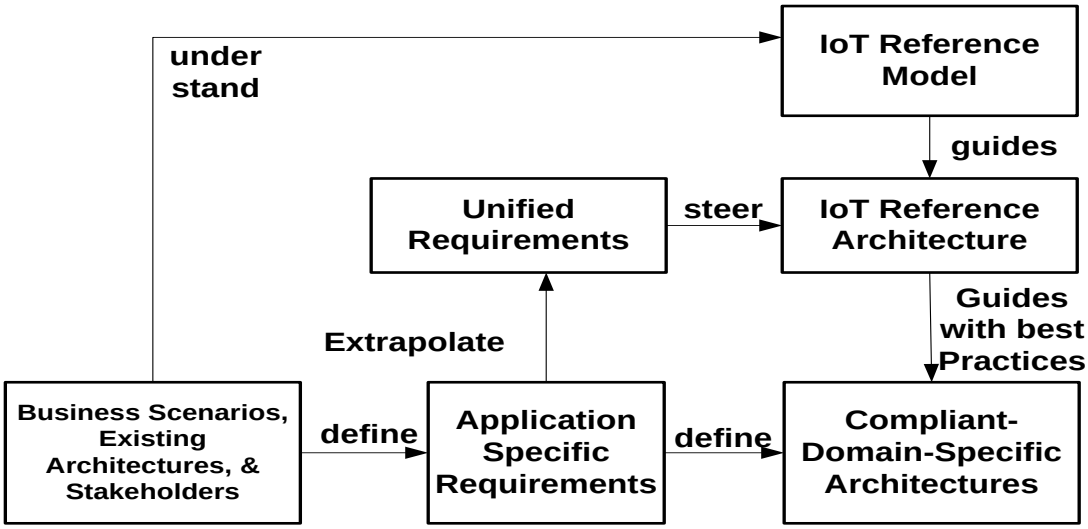

Fig. 4. High Level Design of IoT Reference Architecture [15].

The high-level design of IoT reference architecture is showcased in Fig.4. The backbones of this design level are two important controlling, i.e., i) *dynamic modeling* and ii) *functional modeling*. The first form of modeling results in Reference Model while the second form of modeling assists in Reference Architecture. One interesting feature of IoT architecture is also to provide use cases along with the generation of concrete architectures for a specific application. Another benefit of this architecture is its response system that provides the feedback of inconsistencies (if present within the architecture).

The design of the IoT reference model is carried out using the approach of the Spiral model[16]. The process of abstraction being carried out in higher level with respect to the domain is carried out using industry standard methodology, e.g., SysML [17], Model Driven approach [18], Aspect Oriented approach [19], and Pattern based approach [20]. Out of all these methodologies, Model-driven approach is widely used in the development of IoT architectures. The prime task of Model-driven approach is to transforms any platform independent model to platform-specific model. The aspect-oriented approach is another frequently used methodology in IoT architecture design which performs segregation of all critical supporting functions from the core logic of function in IoT architecture. The pattern-based approach is another frequently selected method in designing IoT architecture. It mainly reutilizes various recursive solutions to sort out generically evolved issues in IoT architecture functionalities. The following Table.1 gives the recently adopted methodologies for IoT architecture.

TABLE I. FREQUENTLY USED THE METHODOLOGY IN IOT ARCHITECTURE

Methodologies	Responsibility
Model-Driven	Transformation for generic to specific architectures
Aspect-oriented	Functionality delineation
Pattern-based	Testing method efficiency

Hence, deployment of IoT architectural model significant uses design patterns to make the implementation lot easier. Therefore the advantages of the use of existing IoT Reference architectural Model are as follows:

- *Cost Effective deployment:* IoT architecture provides a universal ground for multiple IoT system on one single IoT Reference Model.
- *The capability of Cognition:* IoT architectures can provide significant information about the generated architectural robustness.
- *Easier Deployment:* It can generate various specific concrete IoT architectures that make the decision of implementation quite easier.
- *Benchmarking:* The reference model of IoT Architecture can be used as benchmarks for the application specific IoT architectures.

IV. EXISTING SURVEY WORKS IN IOT

This section discusses the existing survey work in the IoT domain to find the proliferation and advancement of research work in the same field. As IoT is one the most interesting research topic, it has attracted various researchers in the past to undergo investigation on the same. There are around 17 review papers associated with IoT issues and advancement; however, the present paper disucsses13 most relevant survey paper on IoT published most recently. However, judging the informative contents of the survey paper was the most difficult one. Hence, we choose to use a Likert scale of 1-5 (1-less information to 5 in more informative) to understand the following informative parameters,

- P_1 represents extents of theoretical discussion
- P_2 represents the extent of the implementation discussion
- P_3 comparative discussion of multiple studies
- P_4 identification of research gap

TABLE II. EXISTING SURVEY WORK ON IOT

Year	Author	P_1	P_2	P_3	P_4
2010	Atzori et al. [21]	5	1	0	0
2010	Yang et al. [22]	5	0	0	0
2013	Aggarwal et al. [23]	5	1	0	0
2013	Said and Masud [24]	3	1	0	0
2013	Perera et al. [25]	4	3	2	1
2014	Whitmore et al. [26]	2	4	0	0
2014	Kumar & Patel [27]	2	2	0	0
2014	Pande & Padwalkar [28]	2	0	0	0
2014	Shah & Ambareen [29]	2	0	0	0
2015	Gazis et al. [30]	2	0	0	0
2015	Botta et al. [31]	3	3	0	0
2015	Fremantle & Scott [32]	2	3	1	0
2015	Karagiannis et al. [33]	2	1	0	0
2016	Bizanis & Fernando [34]	2	3	1	0
2016	Luong et al. [35]	4	4	2	0
2017	Akpakwu et al. [36]	5	3	1	1
2017	Al-Turjman[37]	1	2	0	0
2017	Ni et al. [38]	4	4	1	0
2017	Xu et al. [39]	2	4	1	0
2017	Verma et al. [40]	4	4	1	
2017	Tokognon et al. [41]	2	4	1	0
2017	Sezer et al. [42]	4	3	1	0
2017	Udoh and Kotonya [43]	4	0	0	0
2018	Alioto and Shahghasemi [44]	4	3	1	0
2018	Jeon et al. [45]	2	4	1	0
2018	McKee et al.[46]	1	1	0	0
2018	Saari et al. [47]	1	1	0	0
2019	Benkhelifa et al.[48]	1	2	0	0

The objective of our search for the survey paper was essential to understand the best work done to date in the form of implementation and unsolved problems with respect to the research gap. Table 2 will give a complete highlight of our investigation for existing review papers on IoT.

Table 2 shows that review work done by Perera et al. [25] is the only work to date who have discussed the identification of the research gap. There are only two researchers Fremantle & Scott [32] and Perera et al. [25] found to address the comparative analysis of multiple priorly presented research work. Apart from work done till the year 2015, there is a diversified area on which survey was carried out with respect to IoT. The different categories are software-defined network (Bizanis & Fernando [34]), data aggregation (Luong et al. [35]), 5G (Akpakwu et al. [36]), localization (Al-Turjman [37]), security of fog computing (Ni et al. [38]), clustering techniques (Xu et al. [39]), analytics (Verma et al. [40]), etc. However, more work in focused on communication and its associated performance, but less towards security approaches. All the survey papers published to date has more emphasis on the theoretical aspects of IoT with a lesser context of discussing implementation work by other researchers from the viewpoint of solutions.

V. EXISTING RESEARCH TRENDS

This section discusses the exiting research trends in IoT application. The prime reason for this attempt is to understand what is the scale of the effectiveness of the investigations that have been already made. To adhere to the standard of research manuscript, we investigated the availability of research papers from only reputed international Journals only.

TABLE III. RESEARCH ARCHIVES IN SPRINGER FOR 2010-18

Chapter	71,022
Article	24, 939
Protocols	110
Reference work entry	1134
Book	29
Book Series	1

TABLE IV. RESEARCH ARCHIVES IN SCIENCEDIRECT FOR 2010-18

Year	No. of Journals
2010	2566
2011	2914
2012	3113
2013	3439
2014	4051
2015	4736
2016	5032
2017	6167
2018	5353

Table 3-4 shows the amount of the existing research work being carried out in Springer and ScienceDirect. Reputed IEEE Xplore was found to exhibit the hit of 23,168 manuscripts with the keyword “Internet of Things” published between 2010 and 2018, where there is 18,434 conference paper, 3,889 journals, 551 early access articles, and 275 e-books. With similar keywords, there are 20, 928 journals in Science Direct, 24, 939 Journals on Springer, and 25, 250 journals in ACM Digital Library. The above values are approximated owing to the match with the keywords. The relevancy of the actual content is quite less when appropriately checked with the numbers and abstract of such massive numbers. Below sections and discussion in it will give the correct values of existing research trends in IoT.

A. Frequently Investigated Problems

At present, there is a certain research area which has successfully received the attention of the research communities. This section discusses the problems that have been investigated most frequently in the area of IoT applications.

- *Cloud-based Integration:* Cloud is the prime backbone of the IoT-based applications. Lopez and Macias [49] have carried out a study of IoT framework considering cloud as the major component is the framework. A unique study carried out y Poorter et al. [50] has presented a technique which leverages SOA (Service-Oriented Architecture) of IoT, where cloud services play crucial roles. The study conducted by Mitton et al. [51] has also emphasized on the joint integration of wireless sensors as well as cloud using simulation-based study. Kim et al. [52] have developed another joint integration of cloud and mobile networks using game theory. The studies have also focused on resource allocation dynamically. The significance of virtualization in the cloud has been emphasized by

Abeele et al. [53] by integrating with the sensor network. Hence, there are various archives in reputed journals with more number of publications being focused on the integration of cloud and sensors mainly. However, there are various other computing devices which could also be used to be integrated with the cloud apart from sensors, which has not been focused on existing studies.

- *Data mining Services:* Emphasis on data mining and existing techniques of data mining approaches over IoT can be seen in the most recent review of Chen et al. [54]. This paper has reviewed more than 100 publications that have focused on implementing data mining techniques over cloud integrated with IoT domain. Khan et al. [55] have focused on analytics of large and heterogeneous data over the cloud to be used in IoT applications. Bin et al., [56] have also discussed various research trends on the usage of data mining on IoT applications. The authors have discussed various standard data mining models that are frequently used in IoT. Deployment of semantics in knowledge-extraction process was seen in the study of Bove et al. [57]. The authors have applied it to the RFID based network in IoT. Hachem et al. [58] have studied various schemes of ontologies in IoT. The study has essentially discussed three forms of ontologies used in IoT, i.e., global ontology, device ontology, physics domain ontology, and estimation ontology. Serrano et al. [59] have discussed prominent challenges in IoT with respect to interoperability on semantics. Cretu [60] have presented a semantic web-based application for smart cities of IoT. Hence, numerous studies have repeatedly been investigated in exploring better data mining approaches in IoT.

- *Middleware-based approach:* Integration of large network with numerous devices to capture data is the prime function of IoT, where middleware plays a crucial role in data processing, load balancing, and security management. Work done by Huo et al. [61] has discussed the significance of middleware-based application. Such forms of studies were mainly focused on interoperability and issues associated with the integration of the IoT devices. Lim and Park [62] have developed unique middleware services for performing the sharing of significant resources while integrating cloud and sensors in IoT-based applications. Hachem et al. [63] have introduced a novel middleware system that is motivated by service-oriented architecture in IoT. The middleware was used for mainly governing a large number of the mobile devices in IoT applications.

B. Less Explored Problems

There are few problems in IoT that has been less emphasized in the research area of IoT. Following are some of the problems that have received quite a less attention in the research work.

- *Bandwidth Issues:* It should be noted that 99% of the applications over IoT runs over wireless connectivity. The system allows machine-to-machine communication using existing wireless standards, e.g., Bluetooth, LTE, WLAN, RFID, etc. IoT comprises numerous consumer devices that are connected via the internet. The existing commercial users who depend on wide area network will need to expand their channel capacity soon to fill the gap in bandwidth. At present, the usage of the mobile application, services, and the network is tremendously on the rise and is already creating havoc in traffic management. However, adding to data communication in IoT will further increase the channel capacity, which is quite practically difficult to increase or manage. Moreover, in reality, less than 1% of the available bandwidth existing in the network is being utilized in IoT application. Most recently, the need of larger amount of bandwidth in IoT-based applications is supported by the 3G/4G network. However, it cannot support the integration of the heterogeneous physical devices in IoT, e.g., sensors. The networking and telecommunication services at present don't bear enough capacity to carry the increasing load of traffic of IoT. Bandwidth is one of the significant factors that can potentially impact the performance of IoT applications. The preliminary impact of poor bandwidth will come over data center. Although data centers are there for massive storage, it is not ready for incoming or outgoing data transmission from IoT based applications. It is quite challenging to understand as if 1000 sensors producing data on every one second if IoT comes in commercial usage. Hence, such forms of IoT data transmission may result in high degradation enough to jam the entire services to one data center in 1 day itself. This example is cited only for the sensor network; hence it is almost nightmare to consider other forms of sensing device which captures and transmits data in every second. Hence, although there is massive research work done over conventional bandwidth management system in the normal network as well as cloud, it is essential to emphasize even for IoT also, which has not received considerable attention.

- *Energy Issues:* The IoT devices are majorly low-powered hardware with resource constraint. A closer look into the existing works of literature found that 85% of the existing research work has been focused on using wireless sensor network and rest 15% towards RFID in IoT domain. A battery with limited lifetime powers both the forms of devices (sensors and RFID reader/tags). In a wireless sensor network, it is said that the core design of the sensor is built based on the radio-energy model [64]. According to radio-energy model, it is believed that energy parameter is closely linked with communication in one sensor. This will mean that if the energy dissipates unwantedly than the communication will degrade too thereby reducing the network lifetime of sensors. The biggest problem in IoT pertaining to sensors is related to heterogeneous profiling of its devices. Energy consumption for sensors is quite different from that of the RFID-based device as well as mobile devices. Hence, although at present we have solution towards controlling energy drainage, it is the only applicable inhomogeneous network. No standard

energy aware technique can ensure an efficient controlling of power dissipation. Moreover, such devices are often free from human intervention, which will mean that if the devices are saturated with its battery drainage than there is no way that it can be physically or remotely recharges. Although there is an exception in this case too owing to energy harvesting technologies. However, even energy harvesting technology will require standard external storage and a robust algorithm to decide the need for charging dynamically, when needed. A simple node doesn't have that much memory to execute such complex and sophisticated algorithms. Hence, there is a more significant gap between memory, energy, and computational requirements in IoT devices. Although there is extensive literature approximately 71,117 published between 2010-2018, there are few research implementations towards conserving energy control over IoT-based applications.

- *Security Issues:* Security has always been a constant concern right from the beginning in IoT-based applications. At present, there are more than 10,000 research papers published in the last five years related to security protocols in a wireless network, but very few studies that have proven robust security techniques over IoT-based applications. To enable a better range of security, it is essential that IoT devices must have better access control mechanism, robust and scalable firewall system, effective intrusion detection/prevention system, and potential and fail-proof authentication of IoT devices with secured booting of devices. Researchers have addressed none of these in the last five years or before that. Owing to the inclusion of heterogeneous devices, it is almost impossible to develop a generic algorithm that can provide full-fledged security solutions to the entire ranges of IoT devices. Hence, developing a robust security protocol for 1000 (example) sensors of different types will be a huge expenditure and is quite infeasible owing to integration problems or data processing problems. Moreover, there is no assurity that the developed security protocol can resist the potential threats over the internet, a place where almost every day, thousands of malicious Trojans takes birth and reproduce in the network without even any single alarms. Moreover, there is a bigger trade-off between the security protocols and communication in existing IoT applications. There is a need for the cost-effective solution, which is quite a far from really looking into the existing trends of solutions. Usage of AES, SHA, DES and all form of cryptographic algorithms are already in use, which is already reported of various security threats. Moreover, the dependency of cloud-based services posses another reason for security breaches in IoT applications.

Hence, it is important to understand the extent of research work being carried out in the above three areas in IoT, which have received less attention.

1) Studies on Bandwidth Issue: Bandwidth plays an important role in the communication module of IoT. Table.5 highlights the existing studies in bandwidth issues in IoT. At present, there have been various studies that have focused on bandwidth issues on WLAN [65] along with an emphasis on bandwidth allocation schemes [66]. There are also studies focused on optimizing bandwidth on wireless sensor network [67]. However, studies on bandwidth management in IoT are quite a few to find. This section will discuss 11 research papers that are found to be associated with bandwidth management in IoT. Jin et al. [68] have discussed the emergence of various impediments that calls IoT to possess more work towards bandwidth management. Authors have also theoretically discussed 4 types of architecture, i.e., ubiquitous network, application layer overlay network, autonomous network, service-oriented network. Athreya et al. [69] have presented a technique that allows the devices connected in IoT to organize themselves. The authors have also presented an empirical formulation of self-adaptation with reprogrammable interfaces. The [69] framework analysis and control agent that is connected with radio agent and link agent are given mainly to perform self-organization of IoT devices. In the end, the authors have also discussed the various challenges associated with self-configuration of self-organization of IoT devices. Studies considering the wireless sensor network and its possible involvement in IoT are seen in the work carried out by Zhou et al. [70]. Although the work has focused on minimizing energy consumption among the sensors, the study was performed with a problem identification of bandwidth allocation. The authors have presented simple empirical modeling with outcome tested using energy. Deepalakshmi and Rajaram [71] have introduced a tree-based technique to reserve a good amount of bandwidth in the multistage network like IoT. Xu et al. [72] have addressed the bandwidth problems in an IoT-based multimedia streaming application using delay parameter over the sensor network. The outcome of the study was also compared with a round robin to find reduced computational complexity. Most recently, a research paper of Zachariah et al. [73] has discussed the practical problems of IoT, which is related to the gateway between software and hardware. This problem has a close connection with the IoT for not supporting devices with low-bandwidth. The authors have used the protocol of Bluetooth (IEEE 802.15.4) for profiling gateway. Saeed et al. [74] have presented a novel technique that supports the integration of multiple IoT devices with a focus on task scheduling. Thomas and Irvine [75] have carried out an investigation of bandwidth allocation consider LTE networks as well as the sensor network. Khan et al. [76] have presented a technique for reserving bandwidth over the cloud. The concept is very much close to IoT applications. Jun et al. [77] has developed a scheme for bandwidth allocation for IoT along with cloud using game theory. Yang et al. [78] have discussed the dependencies of the bandwidth factor with respect to IoT based applications. The recent work carried out by Xu et al. [79] has addressed the usage of orthogonal frequency division multiplexing for optimizing the use of bandwidth over noisy channels connected with IoT-device.

2) Studies on Energy Issues: Majority of the devices connected in IoT are operated in low power with batteries, whose lifetime is quite limited. In the existing system, there are various mechanisms that address the issues of energy consumption. There is couple of studies that correlates energy problems with wireless sensor network [80], [81], [82], [83], [84].

Studies concerning the control and management of energy in the viewpoint of IoT applications are less significant in existing works of literature. Table 6 discusses the existing studies on energy management in IoT. Karnouskos [85] have discussed the smart grid applications and discussed the prolonging challenges in IoT. A similar direction of the work is also carried out by Weiss [86]. Sun et al. [87] have presented a scheme that can govern the energy consumption owing to frequent dynamics of the duty cycle with respect to the sensor network. The authors have discussed a greedy technique to accomplish energy conservation. Machado et al. [88] have presented a unique communication protocol in IoT, where the quality of the established link decides the richness of the communication. The study outcome was found with increased packet delivery ratio with energy efficiency. Gorlatova et al. [89] have presented a technique that harvests energy from the kinetic sources on IoT devices. The authors have used real-time prototypes of sensors to perform energy management. Devasenapathy et al. [90] have investigated the possible influence of directionality of antenna as well as energy harvesting on IoT devices. The study introduced a technique to understand the amount of energy required for exploring neighbor nodes. Pabbuleti et al. [91] have essentially investigated some of the prominent security aspects and developed a framework to evaluate the amount of energy required to process it. Usage of WLAN is one of the cost-effective solutions for powering up the low powered devices to IoT. The study introduced by Kellogg et al. [92] is of similar direction. The authors have used real-time Wi-Fi routers to investigate the rate of communication. The performance parameters of the study were tested with the data rate, which is found to decrease with an increase of the distance between the IoT devices and WLAN router. Bin and See [93] have presented a design of control system using a middleware system. Kim et al. [94] have presented a unique framework of energy management for home automation applications in IoT. The study is found to use middle-based approach for conserving energy. The implementation of the study is made over real-time hardware for optimizing power requirements over the photovoltaic panel. Hence, there are various studies that have focused on energy management of the IoT enabled devices in terms of networking. Conserving the maximum amount of residual power is extremely important for IoT enabled applications pertaining to healthcare and industrial automation. Alsaryrah et al. [95] have presented an optimization-based solution towards addressing the energy problems in IoT. Mozaffari et al. [96] have also presented a technique of energy efficiency considering the case study of aerial vehicles. The recent literature by Roy et al.[97] have presented a discussion on sustainable IoT factors where a communication strategy has been presented to support IoT-based communication. Shafique et al. [98] have discussed the importance of energy harvesting in IoT devices using Rectenna-based approach. A complete prototype has been designed and fabricated for this purpose.

TABLE V. EXISTING STUDIES ON BANDWIDTH ISSUES IN IOT

Authors	Techniques	Advantages	Limitation
Jin et al. [68]	Conceptual Discussion about network architectures	Theoretically sound discussion	No focus on implementation
Athreya et al. [69]	Framework for Self-Configuration IoT nodes	Empirical Modelling	No focus on implementation
Zhou et al. [70]	Empirical modeling of bandwidth allocation	Reduced bit-error-rate	The outcome doesn't discuss data delivery, No comparative analysis, and complex computational process due to the iterative method.
Deepalakshmi and Rajaram [71]	Tree-pruning for bandwidth management	Better delay performance	Applicability of this algorithm in the heterogeneous network, e.g., IoT is not discussed.
Xu et al. [72]	Resource allocation, delay-aware	Reduced computational complexity	The study is done considering homogeneous sensor network.
Zachariah et al. [73]	Bluetooth based gateway profiling	Technique supports IoT devices with low bandwidth	Numerical Outcomes and Analysis not discussed in the paper.
Saeed et al. [74]	Task scheduling with bandwidth management	Achieved higher RTT values	Numerical Outcomes and Analysis less focused
Thomas and Irvine [75]	Bandwidth allocation for LTE based sensor network	Better data dissemination by the simulation study	The outcome is measured with packet dropped only.
Khan et al. [76]	Pricing Method to reserve bandwidth	Simple scheduling technique	Applicability of this algorithm in the heterogeneous network, e.g., IoT is not discussed.
Jun et al. [77]	Game theory based resource allocation	Supports cellular network and cloud	Applicability of this algorithm in the heterogeneous network, e.g., IoT is not discussed.
Xu et al. [79]	orthogonal frequency division multiplexing	Enhance data rate	No benchmarking or extensive analysis

TABLE VI. EXISTING STUDIES ON ENERGY ISSUES IN IOT

Authors	Techniques	Advantages	Limitation
Karnouskos [85]	Conceptual discussion	Cost effective Smart Grid design in IoT	Numerical outcomes, benchmarking not discussion
Weiss [86]	Conceptual discussion	-N/A-	Numerical outcomes, benchmarking not discussion
Sun et al. [87]	Decision making for energy control	Reduced duty cycle, good energy conservation	Computational complexity is higher for the greedy approach
Machado et al. [88]	Energy consumption, quality of link-based routing	Reduces energy consumption	Less Applicability on the heterogeneous network
Gorlatova et al. [89]	Energy harvesting technique	Better energy consumption	Computational complexity is higher, no benchmarking
Devasenapathy et al. [90]	Neighbor discovery using the directional antenna	Energy efficient	Scalability issues not addressed
Pabbuleti et al. [91]	Energy minimization for security protocols	Computation overhead optimization	Scalability, benchmarking, complexity not discussed.
Kellogg et al. [92]	The energy requirement for connecting IoT devices with WiFi	Cost-effective solution to reuse WLAN in IoT	Reduction in Data rate, dependability on
Bin and See [93]	Middleware based energy management	Cost effective home automation	Numerical outcomes, benchmarking not discussion
Kim et al. [94]	Middleware based energy management	Better power optimization	Computational complexity is higher, no benchmarking
Alsaryrah et al. [95]	Optimization-based	Energy efficiency	Computational complexity is not carried out
Mozaffari et al. [96]	Energy efficiency	Better trajectory performance	Computational complexity is not carried out
Shafique et al. [97]	Rectenna	Maximum power transmission	No extensive analysis to proof device robustness

3) Studies on Security Issues: Security has always played a critical role in any networking applications and services. For more than a decade there has been extensive research on security protocols, but owing to novelty in the IoT domain, there is an open research question about the success factor of existing security techniques. IoT-based application posses multiple forms of low-powered devices which have their capability of performing encryption and so is its supportability with its connecting network. The biggest challenge in this regards is how to provide a safe encryption mechanism on multiple devices in IoT.

At present, there is already a massive research work being carried out in enabling technologies of IoT, i.e., Wireless Sensor Network, RFID, etc. The recent review work on security issues and challenges involved in secure routing is discussed in [98] [99], while security challenges in RFID based applications are discussed in [100][101][102]. This paper discusses the available research papers that address the security issues in the IoT domain. Katagi and Moriai [103] have presented a discussion on cryptography for securing IoT applications. Khajuria and Andersen [104] have presented a typical encryption technique for securing IoT enabled wireless devices. Developed over FPGA, the authors have used AES (Advanced Encryption Standard) to incorporate security. Yang et al. [105] have adopted PKI (Public Key Infrastructure) and identity-based cryptography for supporting data processing in IoT applications. Saied et al. [106] have presented a security technique using a trust factor for securing communication over IoT domain. The outcome of the study was evaluated with respect to the level of trust in increasing time factor. Kim [107] has presented a unique ciphering scheme at a minimal cost of hardware. Markmann [108] has presented a technique using a smaller length of the digital signature for securing IoT based networks. The study has also used identity-based encryption and outcome is evaluated using energy consumption. Shafagh et al. [109] have adopted homomorphic encryption for promoting privacy on IoT applications. The technique was found to have better compliance of reduced memory usage. Discussion of various standard libraries of encryption is carried out by Kumar et al. [110]. The study has contributed to understanding effective libraries of cryptography to be implemented for securing IoT applications over the internet. Similar usage of homomorphic usage is discussed by Shafagh et al. [111]. Dinu et al. [112] have developed a security framework using block encryption process on real-time ARM processor to testify its effectiveness on IoT applications. Huang and Mu et al. [113] have developed a secure protocol to safeguard RFID-based communication in IoT. The focus of the study was to mitigate forged tag and reader attack, tracking attack, and desynchronization attack using a new distribution of secret key mechanism in cryptography. Hence, it can be seen that there are a good amount of studies that have focused on securing communication over an IoT-based application. The researches formed towards security issues in IoT are given Table.7.

TABLE VII. EXISTING STUDIES ON SECURITY ISSUES IN IOT

Authors	Techniques	Advantages	Limitation
Katagi and Moriai [103]	Cryptographic-based technique	Applicable for low-powered IoT devices	No numerical analysis presented
Khajuria and Andersen [104]	Advanced Encryption Standard	Supports hardware acceleration	No numerical analysis presented
Yang et al. [105]	Public Key Infrastructure, Identity-based Cryptography	Lower algorithm complexity	No numerical analysis presented
Saied et al. [106]	Trust-based security	Resilient against selfish behavior in IoT	Algorithm complexity not discussed, no benchmarking
Kim [107]	Inverse-independent ciphering scheme	Lightweight security protocol	Not resilient against key compromise attacks in IoT
Markmann [108]	Digital Signal, identity-based encryption	Storage compliant,	Not enough validation for security keys
Shafagh et al. [109]	Homomorphic encryption	Lower memory usage	Higher processing time, less extensive analysis of outcome
Kumar et al. [110]	Study of encryption libraries	Good theoretical knowledge about tools	Doesn't have the reflection about its effectiveness on IoT.
Shafagh et al. [111]	Homomorphic encryption	Lower memory usage	Higher processing time, less extensive analysis of outcome
Dinu et al. [112]	block encryption	Lightweight ciphering process	Not resilient against physical attacks in IoT
Huang and Mu et al. [113]	Key distribution	Lightweight ciphering process	No numerical analysis presented

VI. RESEARCH GAP IDENTIFICATION

This section discusses the existing research gap towards IoT. The discussion made in this section is an actual outcome of the review of the literature discussed in prior sections.

- *Less Focus on Bandwidth:* Bandwidth or the channel capacity is one of the critical requirements to make an operational success of existing and upcoming IoT-based applications. The existing studies are more focused on various schemes, but practical implementations and applicability on real-time are still questionable. The literature has less focus on numerical analysis with a few comparative performance analysis, for which reason, existing studies can be just treated as better theoretical guidelines but is quite risky to implement followed by enhancing it. Almost all the studies are done in simulation-based, where there is quite less rationale or justification of the values of parameters with almost no validation of the outcomes. Another bigger problem is an adoption of performance parameters. A better schema of channel capacity will lead to the reduction of propagation delay and increase in throughput. This fact is not found in any outcomes of recent implementations on bandwidth management in IoT.

- *Availability of Energy Conservation Scheme:* The existing studies on energy conservation were found to have various implementations towards energy harvesting schemes mainly related to sensors. However, there was no discussion of any possible connection between energy and communication performance. The standards of wireless sensor networks use first/second order radio-energy model, which means the slightest improvement in energy conservation should also enhance the quality of data transmission and data delivery performance. This phenomenon should be included in the performance assessment of any research work focusing on energy efficiency in IoT. Majority of the prior papers have discussed the usage of sensors but without considering these performance parameters. Moreover, other research gaps explored in the studies pertaining to energy conservation schemes are less applicability on the heterogeneous network, higher computational complexity, no benchmarking, and no addressing of scalability issues.

- *Poor Security Standards:* As discussed, the security systems applied over IoT applications are not able to cater up to the potential vulnerability of the malicious codes that circulates on the internet. Some of the papers discussed that WLAN is one of the cost-effective technology assisting in communications in IoT, but it should be known that WLAN uses security protocols like WEP, WPA, TKIP, etc., which are quite obsolete and all are majorly reported of serious attacks. The existing security techniques used in wireless sensor networks are only developed for securing homogeneous connectivity and never heterogeneous connectivity. Hence, the applicability of existing security standard on multiple IoT devices is not resistive against potential threats in IoT applications and calls for serious investigations.

VII. CONCLUSION

The paper has explored the research trends in IoT applications. The paper starts with briefing the essential characteristics of IoT and various research problems associated with it. From the research analysis it is found that IoT has attracted attention among the research communities, but at the same time, there are also some areas where it has received less focus, e.g., bandwidth, energy conservation, and poor security standards. There is a massive set of research work in all these issues in non-IoT-based applications; however, effective focus

on this with respect to IoT is quite less effective. The paper has explored the hidden problems associated with IoT after reviewing all the significant literature published most recently. With the analysis of the existing researches research problems were incorporated which can be considered for future research. The future work will be towards proposing a novel probabilistic design to schematically parameterize various significant issues in IoT especially emphasizing on channel capacity, energy, and security problems and evolve up design principles to mitigate the issues. In order to accomplish the above mentioned goal, following objectives are targeted viz. i) to apply a probabilistic and strategic decision-making model for signifying the tradeoff between channel capacity and energy efficiency in IoT, ii) to develop an energy-aware trust derivation scheme for securing wireless sensor networks for IoT application, and iii) to provide a method of risk strategy analysis to stimulate the nodes' cooperation thereby minimizing the overhead and maximizing the efficiency suitable for sensors in IoT.

The futuristic scope of the research study is presented as follows

- A system modeling of a novel energy-effective intruder detection and isolation scheme can be analytically designed using robust decision-making principle to address the research gap.
- A simple and yet sophisticated scheme can be formulated for dynamic bandwidth optimization scheme that could offer a higher degree of energy-efficiency.

REFERENCES

[1] O. Vermesan, P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, 2013

[2] F. Behmann, K. Wu, Collaborative Internet of Things (C-IoT): For Future Smart Connected Life and Business, John Wiley & Sons, 2015

[3] M. Aazam, E-N Huh, M.S. Hilaire, "Cloud of things: Integration of IoT with Cloud Computing", *Springer Journal of Robots and Sensor Clouds*, 2015

[4] S. C. Mukhopadhyay, Internet of Things: Challenges and Opportunities, Springer Science & Business Media, 2014

[5] J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, Academic Press, 08-Apr-2014

[6] S. Evdokimov, B. Fabian, O. Gunther, RFID and the Internet of Things: Technology, Applications, and Security Challenges, Now Publishers Inc, 2011

[7] M. Hendry, Near Field Communications Technology and Applications, Cambridge University Press, 18-Dec-2014

[8] M. Henderson, G. Romeo, Teaching and Digital Technologies: Big Issues and Critical Questions, Cambridge University Press, 09-Oct-2015

[9] http://www.jasper.com/iot-service-platform/control-center. Accessed on 20th-Oct, 2015

[10] http://www.arrayent.com/platform/iot-platform-overview/. Accessed on 20th-Oct, 2015

[11] http://aggregate.tibbo.com/solutions/iot-platform.html. Accessed on 20th-Oct, 2015

[12] https://xively.com/. Accessed on 20th-Oct, 2015

[13] https://www.carriots.com. Accessed on 20th-Oct, 2015

[14] https://evrythng.com/. Accessed on 20th-Oct, 2015

[15] M. Bauer, N. Bui, F. Carrez, "Introduction to the Architectural Reference Model for the Internet of Things." Retrieved from http://www.iot-a.eu/public on 20th Oct 2015

[16] A. Bassi, M. Bauer, M. Fiedler, Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model, Springer, 28-Oct-2013

[17] S. Friedenthal, A. Moore, R. Steiner, A Practical Guide to SysML: The Systems Modeling Language, Morgan Kaufmann, 23-Oct-2014

[18] J. Whittle, T. Clark, T. Kuhne, Model Driven Engineering Languages and Systems, Springer- 14th International Conference, 2011

[19] D. Mouheb, M. Debbabi, M. Pourzandi, Aspect-Oriented Security Hardening of UML Design Models, Springer, 22-Apr-2015

[20] S. Balandin, S. Andreev, Y. Koucheryavy, "Internet of Things, Smart Spaces, and Next Generation Networks and Systems", *Springer- 14th International Conference*, 01-Aug-2014

[21] L. Atzori, A. Iera G. Morabito, "The Internet of Things: A survey", *Elsevier-Computer Networks*, vol.54, pp.2787–2805, 2010

[22] D-L Yang, F Liu,Y-D Liang, "A Survey of the Internet of Things", Researchgate-The 2010 International Conference on E-Business Intelligence, 2010

[23] C. C. Aggarwal, N. Ashish, A. Sheth, "The internet of things: a survey

from the data-centric Perspective", Book Chapter in "Managing and Mining Sensor Data", *Springer*, 2013.

[24] O. Said, M. Masud, "Towards Internet of Things: Survey and Future Vision", *International Journal of Computer Networks*, Vol.5, Iss.1, 2013

[25] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey", *IEEE Communications Surveys & Tutorial*, 2013

[26] A. Whitmore, A. Agarwal, L. D. Xu, "The Internet of Things—A survey of topics and trends", *Springer Journal*, 2014

[27] J. S. Kumar, D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", *International Journal of Computer Applications*, Vol.90, No 11, March 2014

[28] P. Pande, A. R. Padwalkar, "Internet of Things –A Future of Internet: A Survey", International Journal of Advance Research in Computer Science and Management Studies, Vol.2, Iss.2, February 2014

[29] P. G. Shah, J. Ambareen, "A Survey of Security Challenges in Internet of Things (IoT) Integration with WSN", Australian Journal of Wireless Technologies, Mobility & Security, 2014

[30] V. Gazis, M. Gortz, M. Huber, "A Survey of Technologies for the Internet of Things", IEEE, 2015

[31] A. Botta, W. Donato, V. Persico, "Integration of cloud computing and Internet of Things: A survey", Future Generation Computer Systems, 2015

[32] P. Fremantle, P. Scott, "A security survey of middleware for the Internet of Things", Open Access of PeerJ Preprints, 2015

[33] V. Karagiannis, P. Chatzimisios, F. V-Gallego, "A Survey on Application Layer Protocols for the Internet of Things", Transaction on IoT and Cloud Computing, 2015

[34] N. Bizanis and F. A. Kuipers, "SDN and Virtualization Solutions for the Internet of Things: A Survey," in IEEE Access, vol. 4, pp. 5591-5606, 2016.

[35] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim and Z. Han, "Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2546-2590, Fourthquarter 2016.

[36] G. A. Akpakwu, B. J. Silva, G. P. Hancke and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," in *IEEE Access*, vol. 6, pp. 3619-3647, 2018.

[37] F. Al-Turjman, "Positioning in the Internet of Things Era: An overview," *2017 International Conference on Engineering and Technology (ICET)*, Antalya, 2017, pp. 1-5.

[38] J. Ni, K. Zhang, X. Lin and X. S. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601-628, Firstquarter 2018.

[39] L. Xu, R. Collier and G. M. P. O'Hare, "A Survey of Clustering Techniques in WSNs and Consideration of the Challenges of Applying

Such to 5G IoT Scenarios," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1229-1249, Oct. 2017.

[40] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama and N. Kato, "A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1457-1477, thirdquarter 2017.

[41] C. Arcadius Tokognon, B. Gao, G. Y. Tian and Y. Yan, "Structural Health Monitoring Framework Based on Internet of Things: A Survey," in *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 619-635, June 2017.

[42] O. B. Sezer, E. Dogdu and A. M. Ozbayoglu, "Context-Aware Computing, Learning, and Big Data in Internet of Things: A Survey," in *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 1-27, Feb. 2018.

[43] I. S. Udoh and G. Kotonya, "Developing IoT applications: challenges and frameworks," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 3, no. 2, pp. 65-72, 6 2018.

[44] M. Alioto and M. Shahghasemi, "The Internet of Things on Its Edge: Trends Toward Its Tipping Point," in *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 77-87, Jan. 2018.

[45] K. E. Jeon, J. She, P. Soonsawad and P. C. Ng, "BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities," in *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 811-828, April 2018.

[46] D. W. McKee, S. J. Clement, J. Almutairi and J. Xu, "Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems," in *CAAI Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 75-82, 6 2018.

[47] M. Saari, A. M. bin Baharudin, P. Sillberg, S. Hyrynsalmi and W. Yan, "LoRa — A survey of recent research trends," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2018, pp. 0872-0877.

[48] E. Benkhelifa, T. Welsh and W. Hamouda, "A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Towards Universal and Resilient Systems," in *IEEE Communications Surveys & Tutorials*.

[49] E. A. Lopez and J A. G Macías, "Mashing up the Internet of Things: a framework for smart environments", *Springer- EURASIP Journal on Wireless Communications and Networking*, vol.79, 2012

[50] E.D. Poorter, I. Moerman and P. Demeester, "Enabling direct connectivity between heterogeneous objects in the internet of things through a network-service-oriented architecture", *Springer- EURASIP Journal on Wireless Communications and Networking*, vol.61, 2011

[51] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S Trivedi, "Combining Cloud and sensors in a smart city Environment", *Springer- EURASIP Journal on Wireless Communications and Networking*, vol.47, 2012

[52] S. Kim, "Nested game-based computation offloading scheme for Mobile Cloud IoT systems", *Springer- EURASIP Journal on Wireless Communications and Networking*, vol.229, 2015

[53] F. V. Abeele, J. Hoebeke, G. K. Teklemariam, "Sensor Function Virtualization to Support Distributed Intelligence in the Internet of Things", *Springer Science-Wireless Personal Communication*, vol.81, pp.1415–1436, 2015

[54] F. Chen, P. Deng, J. Wan, "Data Mining for the Internet of Things: Literature Review and Challenges", *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks*, 2014

[55] Z. Khan, A. Anjum, K. Soomro and M. A. Tahir, "Towards cloud based big data analytics for smart future cities", *Springer-Journal of Cloud Computing, Advances, Systems, and Applications*, Vol.4, Iss.2, 2015

[56] S. Bin, L. Yuan, W. Xiaoyi, "Research on Data Mining Models for the Internet of Things", *IEEE*, 2010

[57] E. Bove, A. Cinquepalmi, D. De Filippis, "A semantic-based framework for RFID-assisted port supply chains", *Toward Emerging Technology for Harbour sYstems and Services*, 2014

[58] S. Hachem, T. Teixeira, V. Issarny, "Ontologies for the Internet of Things", *ACM/IFIP/USENIX* 12th International Middleware Conference, Dec 2011

[59] M. Serrano, P. Barnaghi, F. Carrez, "Internet of Things , *European Research Cluster On The Internet Of Things* ,2015

[60] L-G. Cretu, "Smart Cities Design using Event-driven Paradigm and Semantic Web", *Informatica Economică*, vol. 16, no. 4/2012

[61] C. Huo, T-C Chien, and P H. Chou, "Middleware for IoT-Cloud Integration across Application Domains", *IEEE design and test of computers*, August 2013

[62] Y. Lim and J. Park, "Sensor Resource Sharing Approaches in Sensor-Cloud Infrastructure", *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks*, 2014

[63] S. Hachem. "Service-Oriented Middleware for the Large-Scale Mobile Internet of Things.Mobile Computing". *Universite de Versailles-Saint Quentin en Yvelines*, 2014.

[64] X. Yan, X. Liu, "Evaluating the energy consumption of the RFID tag collision resolution protocols", Springer, Vol. 52, Issue. 4, pp. 2561-2568, 2013

[65] N. Singh, A. K. Singla, "Bandwidth Management in IEEE 802.11 WLAN: A Survey", *International Journal of IT, Engineering and Applied Sciences Research*, Vol.1, No. 1, October 2012

[66] N.Snehalatha, S.A. Julia, P. Rodrigues, "Survey of Bandwidth Management Techniques", *International Journal of Science and Modern Engineering*, Vol.1, Iss.8, July 2013

[67] R. Manjuparkavi, A. Ramya, K. Kalaignanam, P. Sivakumar, "Bandwidth Optimization in Wireless Sensor Networks – A Survey", *Middle-East Journal of Scientific Research*, vol. 23, Iss.7, pp. 1334-1340, 2015

[68] J. Jin, J. Gubbi, T. Luo, and M. Palaniswami, "Network Architecture and QoS Issues in the Internet of Things for a Smart City", *IEEE-International Symposium on Communications and Information Technologies*, 2012

[69] A. P. Athreya, B. DeBruhl, and P. Tague, "Designing for Self-Configuration and Self-Adaptation in the Internet of Things", *IEEE-International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2013

[70] Yang Zhou, Chuan Huang, Tao Jiang, Wireless Sensor Networks and the Internet of Things: Optimal Estimation With Nonuniform Quantization and Bandwidth Allocation, IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013

[71] R. Deepalakshmi, and S. Rajaram, "Effective Heuristic Algorithm For Dynamic Routing And Bandwidth Management Under Quality Of Service Constraints In Multistage Interconnection Networks", *American Journal of Applied Sciences*, vol.11, Iss.3, pp.414-424, 2014

[72] J. Xu, Y. Andrepoulos, Y. Xiao, "Non-stationary Resource Allocation Policies for Delay-constrained Video Streaming: Application to Video over Internet-of-Things-enabled Networks", *IEEE Journal on Selected Areas in Communication*, 2014

[73] T. Zachariah, N. Klugman, B. Campbell, "The Internet of Things Has a Gateway Problem", *ACM*, 2015

[74] A. Saeed, M. Ammar, K. A. Harras, and E. Zegura, "Vision: The Case for Symbiosis in the Internet of Things", *ACM*, 2015

[75] D. Thomas, J. Irvine, "Connection and Resource allocation of IoT Sensors to cellular technology- LTE", *IEEEConference on PhD Research in microelectronics and Electronics*, 2015

[76] A. M. Khan, X. Vilaca, L. Rodrigues, and F. Freitag, "Towards Incentive-Compatible Pricing for Bandwidth Reservation in Community Network Clouds", *GECON*, 2015

[77] H. Jun, Y. Ying, Y. Huifang, "Context-aware resource allocation for device-to-device communications in cloud-centric internet of things, Journal of Chongaing University of Posts and Telecommunication, vol.27, no.4, 2015

[78] W. Yang *et al*., "Narrowband Wireless Access for Low-Power Massive Internet of Things: A Bandwidth Perspective," in *IEEE Wireless Communications*, vol. 24, no. 3, pp. 138-145, June 2017.

[79] T. Xu and I. Darwazeh, "Non-Orthogonal Narrowband Internet of Things: A Design for Saving Bandwidth and Doubling the Number of Connected Devices," in *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2120-2129, June 2018.

[80] J-Y Chang and P-H Ju, “An efficient cluster-based power saving scheme for wireless sensor networks”, Springer- EURASIP Journal on Wireless Communications and Networking, vol.172, 2012

[81] S. K. Gharghan, R. Nordin, and M. Ismail, “A Survey on Energy Efficient Wireless Sensor Networks for Bicycle Performance Monitoring Application”, Hindawi Publishing Corporation Journal of Sensors, 2014

[82] X. Xu, L. Shu, M. Guizani, M. Liu, and J. Lu, “A Survey on Energy Harvesting and Integrated Data Sharing in Wireless Body Area Networks”, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, 2014

[83] G. Zhou, L. Huang, W. Li, and Z. Zhu, “Harvesting Ambient Environmental Energy for Wireless Sensor Networks: A Survey”, Hindawi Publishing Corporation Journal of Sensors, 2014

[84] N. Javaid, M. B. Rasheed, M. Imran, “An energy-efficient distributed clustering algorithm for heterogeneous WSNs”, Springer- EURASIP Journal on Wireless Communications and Networking, vol.151, 2105

[85] S. Karnouskos, “The cooperative Internet of Things enabled Smart Grid”, paper of SAP research, 2010

[86] M. Weiss, “Leveraging residential energy management through the Internet of Things”, ESF Exploratory Workshop on The Internet of Things for a Sustainable Future, Vielsalm, Belgium, May 2011

[87] Z. Sun, C. H. Liu, C. Bisdikian, “QoI-Aware Energy Management in Internet-of-Things Sensory Environments”, IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2012

[88] K. Machado, D. Rosario, E. Cerqueira, “A Routing Protocol Based on Energy and Link Quality for Internet of Things Applications”, Sensors vol.13, pp.1942-1964, 2013

[89] M. Gorlatova, J. Sarik, M. Cong, “Movers and Shakers: Kinetic Energy Harvesting for the Internet of Things”, Technical report of ArXiv, 2013

[90] S. Devasenapathy, R V. Prasad, V. S Rao, “Impact of antenna directionality and energy harvesting rate on Neighbor Discovery in EH-IoTs”, IEEE- Consumer Communications and Networking Conference, 2013

[91] K. Pabbuleti, D. Mane and P. Schaumont, “Energy Budget Analysis for Signature Protocols on a Self-powered Wireless Sensor Node”, Springer Journal, 2014

[92] B. Kellogg, A. Parks, S. Gollakota, “Wi-Fi Backscatter: Internet Connectivity for RF-Powered Devices”, ACM-SIGCOMM, 2014

[93] F. C. Bin, “Energy Awareness Architecture for IoT Home Sensor Network”, The 3rd National Graduate Conference (NatGrad2015), Universiti Tenaga Nasional, Putrajaya Campus, 8-9 April 2015.

[94] J. Kim, J. Byun, D. Jeong, “An IoT-Based Home Energy Management System over Dynamic Home Area Networks”, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, 2015

[95] O. Alsaryrah, I. Mashal and T. Y. Chung, "Bi-Objective Optimization for Energy Aware Internet of Things Service Composition," in *IEEE Access*, vol. 6, pp. 26809-26819, 2018.

[96] M. Mozaffari, W. Saad, M. Bennis and M. Debbah, "Mobile Unmanned Aerial Vehicles (UAVs) for Energy-Efficient Internet of Things Communications," in *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7574-7589, Nov. 2017.

[97] S. S. Roy, D. Puthal, S. Sharma, S. P. Mohanty and A. Y. Zomaya, "Building a Sustainable Internet of Things: Energy-Efficient Routing Using Low-Power Sensors Will Meet the Need," in *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 42-49, March 2018.

[98] K. Shafique *et al.*, "Energy Harvesting Using a Low-Cost Rectenna for Internet of Things (IoT) Applications," in *IEEE Access*, vol. 6, pp. 30932-30941, 2018.

[99] A. Araujo, J. Blesa, E. Romero and D. Villanueva, “Security in cognitive wireless sensor networks. Challenges and open problems”, *Springer- EURASIP Journal on Wireless Communications and Networking*,vol. 48, 2012

[100] F.Mezrag, M.Benmohammed, B.Bouderah, “A Short Survey on Secure Routing Protocols in Hierarchical Cluster-Based Wireless Sensor Networks”, *International Research Journal of Engineering and Technology*, Vol.02, Iss.03, June-2015

[101] I. Erguler, E. Anarim, and G. Saldamli, “A SalientMissing Link in RFID Security Protocols”, *Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking*, 2011

[102] Md Monzur Morshed, A. Atkins and H. Yu, “Secure ubiquitous authentication protocols for RFID systems”, *Springer- EURASIP Journal on Wireless Communications and Networking*, vol.93, 2012

[103] M. Katagi and S. Moriai, “Lightweight Cryptography for the Internet of Things”, 2011. Retreived from https://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf

[104] S. Khajuria and B. Andersen, “Authenticated Encryption for Low-Power Reconfigurable Wireless Devices”, *Journal of Cyber Security and Mobility*, Vol. 1, 189–203., 2012

[105] L. Yang, P. Yu,W. Bailing, “The Internet of Things Security Architecture Based IBE Integration with the PKI/CA”, *SERC*, 2013

[106] Y. B. Saied, A. Olivereau, D. Zeghlache, “Trust management system design for the Internet of Things: A context-aware and multiservice Approach”, *Elsevier-Sciverse ScienceDirect*, vol.1, 2015

[107] H. Kim, K. Kim, “Toward an Inverse-free Lightweight Encryption Scheme for IoT”, CISC-W'14, 2014

[108] T. Markmann, “Securing Constrained Networks with ID-based Cryptography and Short Signatures”, Related Work Report for Amazon WebServices, 2014

[109] H. Shafagh, A. Hithnawi, S. Duquennoy, “Poster: Towards Encrypted Query Processing for the Internet of Things”, *ACM*, 2015

[110] U. Kumar, T. Borgohain, S. Sanyal, “Comparative Analysis of Cryptography Library in IoT”, *International Journal of Computer Applications, International Journal of Computer Applications*, 2015

[111] H. Shafagh, A. Hithnawi, A. Droscher, “Talos: Encrypted Query Processing for the Internet of Things”, ACM SenSys, 2015

[112] D. Dinu, Y. L. Corre, D. Khovratovich, “Triathlon of Lightweight Block Ciphers for the Internet of Things”, ePrints, 2015

[113] P. Huang and H. Mu, “A High-security RFID Grouping Proof Protocol, International Journal of Security and Its Applications”, Vol.9, No.1 pp.35-44, 2015