Exploration on Applications and Challenges of Internet of Things

S.Muthulakshmi Dr.R.Chitra

***Abstract*— With the arrival of smart homes, smart cities, and smart everything, the web of Things (IoT) has emerged as a neighborhood of incredible impact, potential, and growth, with Cisco Inc. predicting to possess 50 billion connected devices by 2020.However, most of those IoT devices are easy to hack and compromise. IoT devices are limited in compute, storage, and network capacity. So that they are easier to attack than other devices like smart phones, tablets, or computers. This paper proposes an in depth overview of the IoT technology and its varied applications in life saving, smart cities, agricultural, industrial etc. Finally some major problems with future research in IoT are identified and discussed in brief.**

***Index Terms*—Architecture, Applications, Challenges IoT and Open Issues.**

I. INTRODUCTION

During the past few years, within the world of wireless communications and networking, a totally unique paradigm named the online of Things (IoT) which was first introduced by Kevin Ashton in the year 1998, has gained more attention within all industries [1]. Unquestionably, the most strength of the IoT vision is that the high impact it'll wear several aspects of every-day life and behavior of potential users. From the purpose of view of a personal user, the foremost obvious effects of the IoT are going to be visible in both working and domestic fields. In this context, assisted living, smart homes and offices, e-health, enhanced learning are only a couple of samples of possible application scenarios during which the new paradigm will play a number one role within the near future [2]. Similarly, from the attitude of business users, the foremost apparent consequences are getting to be equally visible in fields like automation and industrial manufacturing, logistics, business process management, intelligent transportation of people and goods. However, many challenging issues still got to be addressed and both technological also as social knots got to be united before the vision of IoT becomes a reality. The central issues are the thanks to achieve full interoperability between interconnected devices, and therefore the thanks to supply them with a high degree of smartness [3].

The motive of this paper is to spot the breadth, depth and variety of present research in IoT. As a result, enormous number of research publications in journals and conferences are found related to IoT. for instance the continued research work, we filtered the amount of publications from 2013 to 2018 through scopus database. Figure 1 displays the amount of publications in emerging applications of IoT.

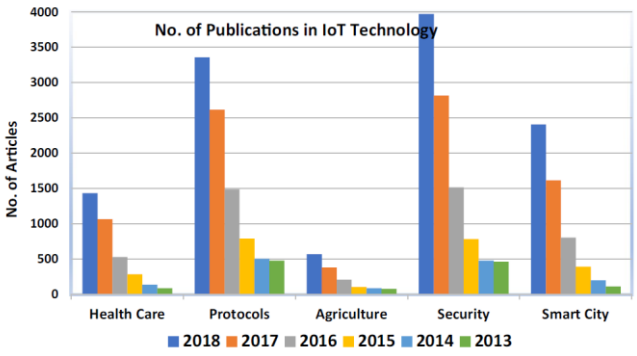

Fig 1 Number of publications in IoT protocols, security and emerging applications

The explosive growth of IoT technology opens many engineering and scientific opportunities and problems. The combined efforts of these sectors should necessarily advent new protocols, architectures, and services which are in dire needs to take up the challenges of IoT. The scopus data base contains large number of publications that use IoT technology for various applications. Table 1 displays the distribution of articles by year wise. It is found from the Table 1 that the number of publications has increased over the recent years and the number rises almost exponentially from 2013 to 2018.

Table 1 Distribution of articles by publication year wise

Year	Number of Articles				
	Health Care	Protocols	Agriculture	Security	Smart City
2018	1433	3357	567	3971	2406
2017	1063	2615	378	2815	1614
2016	526	1487	204	1515	801
2015	282	789	103	782	390
2014	136	501	86	477	197
2013	86	475	75	461	111

The paper is divided as follows; it presents the detailed explanation about IoT architecture in Sect. 2. Section 3 provides review of IoT applications and Sect. 4 discusses about challenges and open issues of IoT applications in

***S.Muthulakshmi**, Computer Science and Engineering, Noorul Islam Centre for Higher Education,Kumaracoil,India (e-mail: masiamuthu@gmail.com).*
***Dr.R.Chitra**, Computer Science and Engineering, Noorul Islam Centre for Higher Education,Kumaracoil,India (e-mail: chitrajegan5@gmail.com).*

detail. Further, it discusses about the future research areas in Sect. 5.Finally Sect. 6 summarizes the paper which concludes this paper.

II. IoT Architecture

Implementation of IoT is predicated on an architecture consisting of several layers: from the field data acquisition layer at rock bottom to the appliance layer at the highest. The layered architecture is to be designed in a way that can meet the requirements of various industries, enterprises, societies, institutes, governments etc. The general architecture of IoT is shown in figure 2 [2]. The layered architecture has two distinct divisions with an online layer in between to serve the aim of a standard media for communication. The two lower layers contribute to data capturing while the 2 layers at the highest is liable for data utilization in applications.

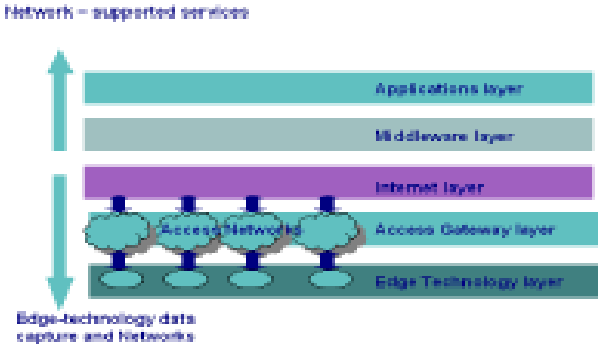

Fig 2 Layered architecture of Internet of Things

The functionalities of the numerous layers are discussed briefly within the following:

Edge layer: There are sensor networks, embedded systems, RFID tags and readers or other soft sensors in this layer. These entities are the primary data sensors deployed within the field.Many of these hardware elements provide identification and knowledge storage (e.g. RFID tags), information collection (e.g. sensor networks), information science (e.g. embedded edge processors), communication, control and actuation.

Access gateway layer: The first stage of knowledge handling happens at this layer. It performs message routing, publishing and subscribing and also performs cross platform communication.

Middleware layer: this is often often one of the foremost critical layers that operate in bidirectional mode. It acts as an interface between the hardware layer at the lowest and thus the appliance layer at the very best . It is liable for critical functions like device management and knowledge management and also takes care of issues like data filtering, data aggregation, semantic analysis, access control, information discovery.

Application layer: This layer at the highest of the stack is liable for delivery of varied applications to different users in IoT. The applications are often from different industry verticals such as: manufacturing, logistics, retail, environment, public safety, healthcare, food and drug etc.

III. Applications of IoT

The potentialities offered by the IoT make it possible to develop numerous applications supported it, of which only a couple of applications are currently deployed. There will be many different applications in future for different fields. In the following subsections, a number of the important example applications of IoT are briefly discussed.

Smart Environment: Smart environment includes various IoT applications such as fire detection in forests, monitoring the level of snow in high altitude regions, preventing landslides, early detection of earthquakes, pollution monitoring, etc. All these IoT applications are closely associated with the lifetime of citizens and animals in those areas. The government agencies involved in such fields also will be counting on the knowledge from these IoT applications.

Aerospace and aviation industry: IoT can help to enhance safety and security of products and services by reliably identifying counterfeit products and elements. The aviation industry, for instance, is susceptible to the matter of suspected unapproved parts (SUP). SUPs seriously violate the safety standards of an aircraft. Aviation authorities report that at least 28 accidents or incidents in the United States have been caused by counterfeits [3].

Smart Cities: Smart cities involve extensive use of emerging computation and communication resources for increasing the overall quality of life of the people[4].It includes smart homes, smart traffic management, smart disaster management, smart utilities, etc. There is a push to make cities smarter, and governments worldwide are encouraging their development through various incentives [5]. Although the use of smart applications is intended to improve the overall quality of life of the citizens, it comes with a threat to the privacy of the citizens. Smart card services tend to put the card details and purchase behavior of the citizens at risk. There will be a chance of leaking the user's location in smart mobility applications. There are applications using which parents can keep track of their child. However, if such applications are hacked, then the safety of the child can come to risk.

Smart Agriculture: The rules to trace the agricultural animals and their movements require the utilization of technologies like IoT, making possible the important time detection of animals, for instance during outbreaks of contagion . Moreover, in many cases, countries give subsidies counting on the amount of animals during a herd and other requirements, to farms with cattle, sheep, and goats [6]. As the determination of the amount is difficult, there's always the likelihood of frauds. Good identification systems can help minimize this fraud. Therefore, with the appliance of identification systems, animal diseases are often controlled, surveyed, and prevented [15]. To certify the health status of regions and countries by using IoT, the blood and tissue specimens should be identified accurately. With the web of Things, single farmers could also be ready to deliver the crops on to the consumers not only during a small region like in marketing or shops but in a wider area. This will change the entire supply chain which is especially within the hand of huge companies, now, but can change to a more direct, shorter chain between producers and consumers.

Security and Emergencies: Security and emergencies is another important area where various IoT applications are being deployed. It includes applications such as allowing only authorized people in restricted areas etc [9]. Another application in this domain is the detection of leakage of hazardous gases in industrial areas or areas around chemical factories. Radiation levels can also be measured in the areas around nuclear power reactors or cellular base stations and alerts can be generated when the radiation level is high. There are many buildings that have sensitive data or sensitive goods. Security applications are often deployed to guard sensitive data and goods [12]. IoT applications that detect various liquids also can be wont to prevent corrosion and break downs in such sensitive buildings. Security breaches in such applications also can have various serious consequences. For example, the criminals may try to enter the restricted areas by attacking the vulnerabilities in such applications. Also, false radiation level alarms can have serious immediate and future impacts[10]. For example, if infants are exposed to high levels of radiation, then it may lead to serious life threatening diseases in long term.

IV. CHALLENGES AND OPEN ISSUES IN IOT

The work flows in analyzed enterprise environment, home, office and other smart spaces in the future will be characterized by cross organization interaction, requiring the operation of highly dynamic and ad-ho relationships [7]. There are very limited ICT support is available at present, and the following key challenges exist.

(i) Network Foundation - mobility, availability, manageability and scalability are the main barriers to IoT [8].

(ii) Security, Privacy and Trust - within the domain of security the challenges are:

(a) Securing the architecture of IoT - security issues should be solved at design time and execution time.(b) Proactive identification and protection of IoT from arbitrary attacks (e.g. DoS and DDoS attacks) and abuse.(c) Proactive identification and protection of IoT from malicious software.

In the domain of user privacy, the specific challenges are: (a) data privacy and location privacy (b) Standards, methodologies and tools for identity management of users and objects.

(c) privacy enhancement technologies and relevant protection laws are required.

In the domain of trust, a number of the specific challenges are: (a) Need for straightforward and natural exchange of critical, protected and sensitive data - e.g. smart objects will communicate on behalf of users / organizations with services they will trust [11]. (b) Trust has got to be a neighborhood of the planning of IoT and must be built in.

(iii) Managing heterogeneity - managing heterogeneous applications, environments and devices constitute a serious challenge. In addition to the above major challenges, some of the other challenges are: (a) Managing large amount of information and mining large volume of data to provide useful services [13].(b) Designing an efficient architecture for sensor networking and storage (c) Designing mechanisms for sensor data discovery (d) Designing sensor data communication protocols - senor data query, publish/subscribe mechanisms (e) Developing sensor data stream processing mechanisms [14].(f) Sensor data mining - correlation, aggregation filtering techniques design. Finally, standardizing heterogeneous technologies, devices, application interfaces etc. will also be a major challenge.

Open issues of emerging applications are listed in Table 2.

Table 2 some open issues for emerging applications of IoT

S. No	Application	Some Open Issues/Areas
1	Agriculture	Health status of agricultural stocks, crops Supply chain management to bridge between demand and supply Forecasting weather conditions and protection of fields Integration of machinery with technology, protocols, communication etc.
2	Industry	Product life cycle and production control Smart sensing Solutions for latency and reliability mechanism Energy consumption and bandwidth
3	Smart city	Crowd monitoring and Guidance Threats, security and methodology for resilience to faults and Waste management and transportation Mobility management
4	Health	IoT for new diseases and disorders Nutrition management systems and devices Flexible electronics and mechanical devices Ambient assisted living

V. FUTURE RESEARCH AREAS

There are several areas during which further research is required for creating deployment of the concept of IoT reliable, robust and efficient. Some of the areas are identified in identification technology domain, development of latest technologies that address the worldwide ID schemes, identity management, identity encoding/ encryption, pseudonimity, revocable anonymity, party authentication, repository management, authentication and addressing schemes. Therefore the creation of worldwide directory lookup services and discovery services for IoT applications with various identifier schemes. In communication protocol domain, the problems that require to be addressed are: design of energy efficient communication by multi frequency protocol, communication spectrum and frequency allocation, software defined radios to remove the requirements for hardware upgrades for brand spanking new protocols, and style of high performance, scalable algorithms and protocols. In network technology domain further research is required on chip technology considering on chip communication architectures for dynamic configurations design time parameterized architecture with a dynamic routing scheme and a many number of allowed virtual connections at each output.

VI. CONCLUSION

In this paper I have discussed the layered architecture of Internet of Things in detail. Also discussed about the various applications of IoT and the number of publications in the area of IoT. Various open issues of present IoT applications also have been discussed. We have also discussed about the future research areas of IoT. This survey is expected to serve as a valuable resource for security enhancement for upcoming IoT applications.

REFERENCES

[1] G. Santucci. From Internet to Data to Internet of Things. Proceedings of the International Conference on Future Trends of the Internet. (2009).

[2] L. Atzori, A. Lera, and G. Morabito. The Internet of Things: A Survey. Computer Networks 54(15), 2787-2805. (2010).

[3] CTV Deadly Fakes- CTV News. Url:http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20020306/ctvnews848463

[4] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, ''Smart cities: A survey on datamanagement,security,andenablingtechnologies,''IEEECommun.SurveysTuts., vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[5] D. Eckhoff and I. Wagner, ''Privacy in the smart city—Applications, technologies, challenges, and solutions,'' IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 489–516, 1st Quart., 2018.

[6] Soumyalatha, S. G. H. (2016). Study of IoT: Understanding IoT architecture, applications, is-sues and challenges. In 1st International conference on innovations in computing and net-working (ICICN16), CSE, RRCE. International journal of advanced networking and applications.

[7] Liu, Y., Seet, B. C., & Al-Anbuky, A. (2013). An ontology-based context model for wireless sensor network (WSN) management in the Internet of Things. Journal of Sensor and Actuator Networks, 2(4), 653–674.

[8] N. N. Dlamini and K. Johnston, ''The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review,'' in Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE), Nov. 2016, pp. 430–436.

[9] Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In 2017 IEEE international systems engineering symposium (ISSE), IEEE, pp. 1–7.

[10]Kumar, S., Poddar, S., Marimuthu, R., Balamurugan, S., & Balaji, S. (2017). A review on communication protocols using internet of things. In 2017 International conference on microelectronic devices, circuits and systems (ICMDCS), IEEE, pp. 1–6.

[11]Sanchez-Iborra, R., & Cano, M. D. (2016). State of the art in LP-WAN solutions for industrial IoT services. Sensors, 16(5), 708.

[12]Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. International Journal of Production Research, 56(8), 2941–2962.

[13]Calabretta, M., Pecori, R., & Velti, L. (2018). A token-based protocol for securing MQTT communications. In 2018 26th International conference on software, telecommunications and computer networks (SoftCOM), IEEE, pp. 1–6.

[14]Dalkiltc, G. (2018). Authentication and authorization mechanism on message queue telemetry transport protocol. In 2018 3rd International conference on computer science and engineering (UBMK), IEEE, pp. 145–150.

[15]Al-Fuqaha, A., Khreishah, A., Guizani, M., Rayes, A., & Mohammadi, M. (2015). Toward better horizontal integration among IoT services. IEEE Communications Magazine, 53(9),72–79.

S.Muthulakshmi received BE degree in Computer Science and Engineering from Anna University, India and ME in Software Engineering from Visvesvaraya Technological University, India.Doing Ph.D in Noorul Islam Centre for Higher Education in Computer science and Engineering.Research interest includes IoT Security, Blockchain.

R.Chitra, received the BE degree in Electrical and Electronics Engineering, ME and PhD degree in Computer Science and Engineering from Manonmaniam Sundaranar University, India. She is currently working as an Associate Professor at Noorul Islam Centre for Higher Education in the Department of Computer Science and Engineering.. Her research interests include datamining, intelligent techniques and softcomputing.