ISSN: 2278-4632
Vol-10 Issue-6 No. 18 June 2020

Impact of Statistical Tools on Internet of Things (IoT): An Analysis

Dr Manpreet Kaur, Assistant Professor,
GGS College, Sector 26 Chandigarh, Email- preetbhullar82@gmail.com

Mr Harpreet Singh, Assistant Professor, GGS College, Sector 26 Chandigarh

Abstract: The trend of Internet of Things (IoT) has created an urge in the field of technology to develop smart life with the help of smart gadgets. Internet plays a crucial role in such kind of development. IoT guarantees to make living easier and protected with its numerous applications. Like other technologies, it also has certain shortcomings of connectivity, privacy of data, resources utilisation, limited battery devices for mobile connectivity and technology. This paper explores some of the factors affecting IoT adoption, analyzing the determinants and other challenges. In order to acquaint researchers with the increasing trend in this field, this paper finally illustrates the developing trend of IoT projects and reveals how IoT has affected research work by investigating IoT growth in various sub-domains. A statistical analysis is also illustrated in this paper to throw a glance on deployment of IoT in the field of technology.
Keywords: Internet of Things (IoT), Statistics, IoT challenges

I. Introduction

The new era of computing has lead to overcome various traditional methods that were deployed. The drift from wired medium to wireless, has gained an exposure to safeguard data and retain communication without any drop-off. Wireless networks created a research opportunity in the field of data security, network establishment, faster access to data, consistent computation and many others. People across the globe are working in this path to create digital communication a boom for the industry. As no successful research can be attained without overcoming certain hurdles, so smart connectivity of IoT has also emerged as a stone in milestone. Internet of Things (IoT) methodology allows devices to get connected to each other which must be surrounded by network in one form or another.

The IoT is regarded as the next phase in the evolution of the internet. It will enable commonplace devices to be connected to the internet to achieve many disparate goals. With potentially billions of devices to be connected, it is clear that standardization will be required in order to avoid chaos. One estimate is that only 0.6% of objects that could be part of the IoT are currently connected. By 2020, there could be up to 50 billion devices connected to the internet, far greater than the number of human users[1].

Internet of Things (IoT) has rapidly elevated into one of the emerging fields in cellular communication and pervasive computing. IoT has wide coverage from indoor networks to outdoor networks, for example Wide Area Network (WAN)/5G. IoT devices are diversified and differ by means of power consumption, signal transmission, networking ability, and battery life. Despite their diversity and individual features, IoT applications having the basic

ISSN: 2278-4632
Vol-10 Issue-6 No. 18 June 2020

issues which require to be fixed by the right algorithms within the specific contexts. For instance, the adaptation of algorithms, the effective use of resource, drift control, and network coverage have a wide application in IoT for the reasons such as utilization of resource, networking, partnership and management. IoT transmissions provide key scope to design accurate, economical, reasonable-power, dependable, and scalable solutions for cutting-edge applications.[2]

Certain issues arise with implementation of IoT which need to be addressed in this paper. For effective and error free execution of services in IoT, one must ensure proper communication in the networks. Every machine attached in the network must establish a proper connection with the internet. These devices are free to collect different types of data with their internal sensing and monitoring environment. Architecture standardization is also treated as another issue in IoT. With the changing era of technology, there must be adaptation of IoT as per challenges faced day to day. As most of the mobile devices connected have limited battery support, so energy efficiency also accounts for another issue in this domain. When the data is transmitted in the network, trust issues arise. Security and Privacy of data need to be addressed in IoT. They act as a critical issue to measure performance and management.
This paper is further organized in following sections where Section II focuses on IoT in deatil, considering its issues, background and applications respectively. Section III depicts statistic analysis of studies conducted in different fields of IoT. In Section IV, the paper presents conclusion and future scope.

II. IoT in Detail

The internet of things (IoT) is the network of physical devices, vehicles, buildings and alternative things embedded with physical science, software, sensors, actuators, and network property that modify these objects to collect and exchange data. In 2013 the world Standards Initiative on internet of Things (IoT-GSI) outlined the IoT as "the infrastructure of the data society. The IoT permits objects to be detected and controlled remotely across existing network infrastructure, creating opportunities for heaps of direct integration of the physical world into computer-based systems, and ensuing in improved efficiency, accuracy and economic benefit. When IoT is increased with sensors and actuators, the technology becomes an instance of the a lot of general category of cyber-physical systems, that conjointly encompasses technologies like sensible grids, smart homes, intelligent transportation and smart cities. Each factor is unambiguously diagnosable through its embedded automatic data processing system however is in a position to interoperate among the present internet infrastructure. Experts estimate that the IoT can incorporate virtually fifty billion objects by 2020.[3]
In this section, four aspects about each IoT features are elaborated: description, threat, challenges, solutions and opportunities.[4]
1). *Description*: What the feature is and what the differences between traditional devices, network and applications are.
2).*Threat*: What potential threats and vulnerabilities brought by the feature, and the consequences caused by these threats. It also provide diagrams and attack examples for some threats, which makes it easy to follow.

ISSN: 2278-4632
Vol-10 Issue-6 No. 18 June 2020

3). *Challenges*: What research challenges caused by the features.
4). *Solutions & Opportunities*: Existing solutions to tackle the challenges and the drawbacks of these solutions.

The Internet of things applications or more is extremely fascinating which gives advances to savvy each thing, yet there are a few difficulties to the utilization of the Internet of Things idea in cost of execution. The desire that the innovation must be accessible requiring little to no effort with countless. IoT are likewise looked with numerous different difficulties [5], for example,

- *Scalability*: Internet of Things has a major idea than the traditional Internet of PCs, on account of things are coordinated inside an open domain. Fundamental usefulness, for example, correspondence and administration revelation in this manner need to work similarly effectively in both little scale and substantial scale situations. The IoT requires another capacities and strategies keeping in mind the end goal to pick up a proficient task for versatility.
- *Data Interpretation*: To help the clients of keen things, there is a need to translate the neighborhood setting dictated by sensors as precisely as could be expected under the circumstances. For specialist organizations to benefit from the divergent information that will be created should have the capacity to reach some generalizable inferences from the deciphered sensor information.
- *Interoperability*: Each kind of brilliant protests in Internet of Things have diverse data, preparing and correspondence abilities. Distinctive keen articles would likewise be subjected to various conditions, for example, the vitality accessibility and the correspondences data transfer capacity prerequisites. To encourage correspondence and participation of these articles, basic guidelines are required.
- *Automatic Discovery*: In powerful conditions, reasonable administrations for things must be naturally recognized, which requires proper semantic methods for portraying their usefulness.
- *Software Complexity*: A more broad programming foundation will be required on the system and on foundation servers with a specific end goal to deal with the brilliant protests and give administrations to help them. that in light of the fact that the product frameworks in brilliant articles should work with insignificant assets, as in ordinary implanted frameworks.
- *Adaptation to non-critical failure*: Objects in web of things is considerably more unique and versatile than the web PCs, and they are in changing quickly in sudden ways. Organizing an Internet of Things in a strong and dependable way would require repetition on a few levels and a capacity to consequently adjust to changed conditions.
- *Power supply*: Things ordinarily move around and are not associated with a power supply, so their brilliance should be controlled from an independent vitality source. Albeit latent RFID transponders needn't bother with their own particular vitality source, their usefulness and interchanges go are extremely restricted. Expectations are stuck on future low power processors and correspondences units for inserted frameworks that can work with essentially less vitality. Vitality sparing is a factor in equipment and framework engineering, as well as in programming, for instance the

ISSN: 2278-4632
Vol-10 Issue-6 No. 18 June 2020

execution of convention stacks, where each and every transmission byte should legitimize its reality.

- *Security and Privacy*: notwithstanding the security and assurance parts of the Internet such in correspondences secrecy, the legitimacy and reliability of correspondence accomplices, and message respectability, different necessities would likewise be vital in an Internet of Things. There is a need to get to specific administrations or keep from speaking with different things in IoT and furthermore business exchanges including savvy articles would ought to be protected from contenders' nosy eyes.

These challenges are addressed in the paper, still leads to growing trend in usage of IoT projects worldwide.

III. Statistical Analysis

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.[6]

The papers on which analysis is done are combined papers that possess similar pattern of domains. The main aim of this study is to promote trending of IoT over other domains. Multiple researchers are working in this field while some students are observing its rapidly growing evolution.

As per the investigations, it can be observed that the research in IoT domain is in trend and multiple fields are clubbing with it to promote technology efficiently. The fields that posed to be sub-domains can be classified as Trust management, software services, technology and so on. To increase the performance, numerous supporting technologies can also be utilised.

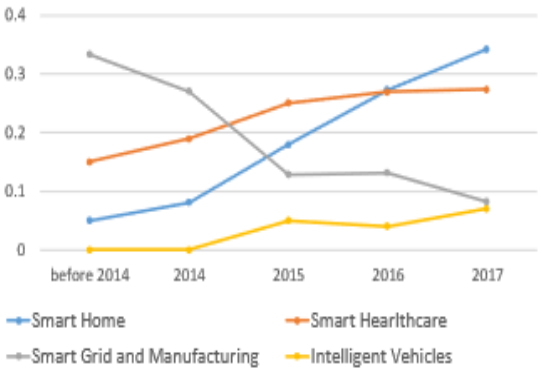

Figure1: Proportion of Number of papers in Different Applications per year.[4]

Figure 1 illustrates the modification of the proportion of the number of papers in some application scenarios in recent years. IoT security research hotspot always follows the development of IoT applications. However, with the rapid development of smart home and healthcare technology over the last three years, security researchers turned more attention to

ISSN: 2278-4632
Vol-10 Issue-6 No. 18 June 2020

these field, at the same time, the research interests in the smart grid and smart manufacturing was on the decline.

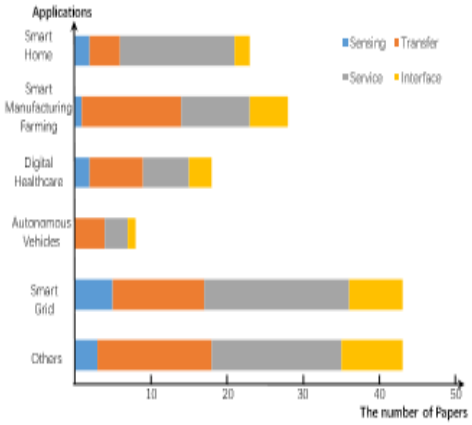

Figure 2: Number of Papers in each Layer in Different IoT Application[4]

Figure 2 depicts the number of research papers in each layer of every IoT application scenario. It can be observed that security studies distribution of different layers varied from one application scenario to another. The security problems in WSN will be more dangerous to others. Smart home devices are controlled by mobile applications or web applications. Therefore, more researchers drew more attention to application security in smart home and transfer security in smart manufacturing.

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.[6]

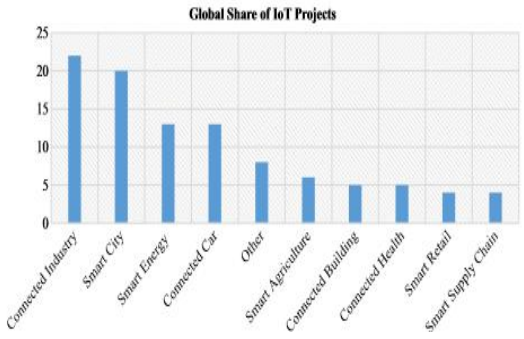

Figure 3: Global share of IoT Projects across the world[9]

ISSN: 2278-4632
Vol-10 Issue-6 No. 18 June 2020

In figure 3, the global share of IoT projects are depicted across the globe. It can be seen that smart city projects are second highest in demand as compared to connected industry. Whereas, smart supply chain holds the least percentage of projects developed worldwide.

IV. Conclusion and Future Scope

This paper analyzed and discussed the issues that are addressed of IoT features. This may lead to certain threats and research challenges which evolve from these features. Then, existing solutions are proposed for these challenges and stated the aspects of IoT features further. Finally, the development trend of recent IoT research have been statistically analysed and depict how IoT features reflect on the existing research field. The papers also focussed on which analysis is done are combined papers that possess similar pattern of domains. The main aim of this study was to promote trending of IoT over other domains and is depicted graph wise with the help of statistics.

References

1. Ryan, P.J., Watson, R.B.," Research Challenges for the Internet of Things: What Role Can OR Play?", Systems 2017, Volume 5, Issue 24, March 2017.
2. Ayesha Ijaz et al., “Enabling massive IoT in 5G and beyond systems: PHY radio frame design considerations”, IEEE Access, Vol. 4.
3. Selvaraj, D., Bharathiraja, R., Gokul Nath, V. , Immanuel, E., Jyothesvar G. L.," Iot Based Traffic Congestion Monitoring And Management System", International Research Journal of Engineering and Technology (IRJET), Volume 05, Issue 09, September 2018.
4. Zhou, W., Zhang, Y., Liu, P.," The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE, January 2018.
5. Pote, S. V., Jadhav, B. D.," Internet Of Things Applications, Challenges And New Technologies", Proceedings of International Conference on Advances in Computer Technology and Management (ICACTM), pp. 45-51, February, 23rd and 24th, 2018.
6. Rouhifar, M., Bahramzadeh, S., Hedayati, A., Aghazarian, V., Chahardoli, M." Statistical Analysis on IoT Research Trends: A Survey", J. ADV COMP ENG TECHNOL, Volume 4, Issue 2, Spring 2018.
7. Lin, Jie, et al. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications." IEEE Internet of Things Journal., vol. 99, p1 2017.
8. R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed Internet of Things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
9. IoT application areas," https ://iot-analy tics.com/top-10-iot-proje ct-appli catio n-areas -q3-2016/", Apr 2019.
10. Jaydip Sen," Security and privacy issues in cloud computing", Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India. https://arxiv.org /ftp/arxiv /papers/1303/1303.4814.pdf
11. Saranya C. M., Nitha K. P., "Analysis of Security methods in Internet of Things", International Journal on Recent and Innovation Trends in Computing and Communication, Volume 3, Issue 4, April 2015.
12. Sophia Antipolis," New ETSI specification for Internet of Things and Machine to Machine Low Throughput Networks", 30 September 2014. http://www.etsi.org/news-events/news/827-201409-news-etsi-new-specification-for-internet-of- things-and-machine-to-machine-low-throughputnetworks.
13. http://www.cloud-council.org/deliverables/CSCCCloud-Security-Standards-What-to-Expect-andWhat-to-Negotiate.pdf