IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Internet Of Things (Iot): A Literature Review

Dr. Manju Sharma, Assistant Professor
Department of Computer Science, College of Engineering & Computer Science,
Jazan University, Jazan, Kingdom of Saudi Arabia

Abstract:

Nowadays, the world has witnessed a drastic change towards modern technology and how much it has advanced, even the specialized companies are undergoing through a major transformation in the field of information technology, specifically in the Internet of Things (IoT). This paradigm shift or IoT refers to the integration of physical objects with the internet and digital technologies through the addition of hardware and software, enabling these objects to become smarter and easier to work with. It allows them to communicate with one another and interact effortlessly with other people, supporting the various aspects of everyday life. As a result, it supports the new forms of interaction between humans and devices and even includes inter device communication among each other —which ultimately revolutionizes traditional lifestyles into something that's more seamless and high techdespite the major progress , this evolution does have several obstacles . Before achieving the full benefits of Iot we have to overcome the technical, social and ethical issues. The key purpose of this review paper is to offer readers an in-depth analysis from both technological and societal viewpoints. It includes exploring the key challenges and concerns that are linked to IoT, along with its interpretation providing a clear description of iot and architectural structure.

Furthermore, this paper emphasizes range of sensors and actuators that are involved in IoT systems and their role in fostering smart communication. The paper highlights the most critical applications areas in Iot.

The purpose of this study is to provide the readers with more profound understanding of Iot and its impact on the real world

Index Terms

Internet of things (IoT), IoT Ecosystem , Smart Communication, Sensors, Actuators, System integration, Network interface

Introduction

'If we want to define IOT then we cannot define it precisely and concisely but Vermesan et al. defined the Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators [10].

The rapid development of the Internet of Things (IoT) and services it offer have made it the fastest growing technology. Internet of Things (IoT) devices becoming ubiquitous and pervasive. IOT success has not gone unnoticed but the threats and attacks in IoT devices and services are increasing day by day. It is an idea that could alter our relationship with technology.

‘The term “Internet of Things” (IoT) was coined by Kevin Ashton at a presentation to Proctor & Gamble in 1999. He is one of the founders of the Massachusetts Institute of Technology’s Automatic Recognition Lab. He pioneered RFID (used in barcode detector) technology in the field of supply chain management. He also founded Zensi, a company that manufactures energy sensing and monitoring technologies.

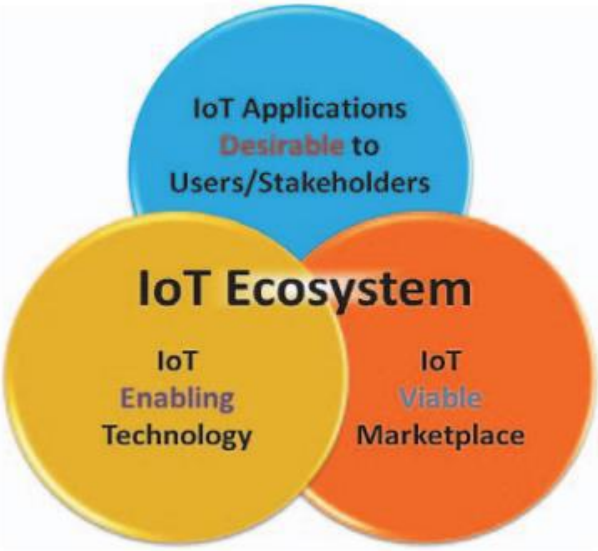

Figure 1: IoT Ecosystem.

The Internet of Things is an emerging topic of technical, social and economic importance. Consumer products, durable goods, cars and trucks, industrial components and facilities, sensors, and other everyday objects are combined with internet connectivity and powerful data analysis capabilities that promise to transform the way we live and work. A major shift in our daily routines can be observed along with the widespread implementation of IoT devices and technologies. IoT is everywhere, although we don’t always see it or know that a device is part of it. For consumers, new IoT products like Internet-enabled devices, home automation components and power management devices drives us toward seeing “Smart home”, which provides more safety and energy efficiency. Other IoT personal devices such as wearable fitness and health monitors that support the network-enabled medical devices are transforming the way healthcare services are delivered. The Internet of Things transforms physical objects into an information ecosystem shared between wearable, portable, and even implantable devices, making our life technology and data rich.’[1]

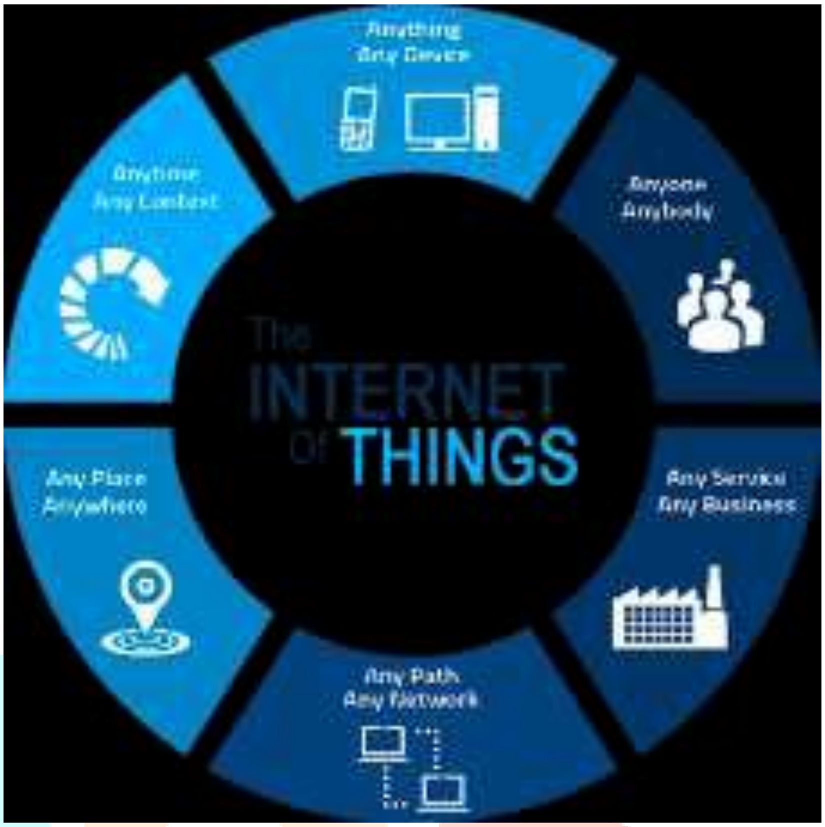

Fig -2: Definition of IoT[11]

‘The recent rapid development of the Internet of Things (IoT) and its ability to offer different types of services have made it the fastest growing technology, with huge impact on social life and business environments. Internet of Things (IoT) devices are rapidly becoming ubiquitous while IoT services are becoming pervasive. Their success has not gone unnoticed and the number of threats and attacks against IoT devices and services are on the increase as well.’[2]

‘CHARACTERISTICS OF INTERNET OF THINGS (IOT)

Some most popular characteristics of Internet of things are:
(a) Intelligence
(b) Connectivity
(c) Dynamic Nature
(d) Enormous scale
(e) Sensing
(f) Heterogeneity
(g) Security

(a) Intelligence

IoT comes with the combination of algorithms and computation, software & hardware that makes it smart. Ambient intelligence in IoT enhances its capabilities which facilitate the things to respond in an intelligent way to a particular situation and supports them in carrying out specific tasks. In spite of all the popularity of smart technologies, intelligence in IoT is only concerned as means of interaction between devices, while user and device interaction is achieved by standard input methods and graphical user interface [8]. Together algorithms and compute (i.e. software & hardware) provide the “intelligent spark” that makes a product experience smart. Consider Misfit Shine, a fitness tracker, compared to Nest’s intelligent thermostat. The

Shine experience distributes compute tasks between a smartphone and the cloud. The Nest thermostat has more compute horsepower for the AI that make them smart.

(b) Connectivity

Connectivity empowers Internet of Things by bringing together everyday objects. Connectivity of these objects is pivotal because simple object level interactions contribute towards collective intelligence in IoT network. It enables network accessibility and compatibility in the things. With this connectivity, new market opportunities for Internet of things can be created by the networking of smart things and applications. Connectivity in the IoT is more than slapping on a WiFi module and calling it a day. Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data. If this sounds familiar, that's because it is Metcalfe's Law and it rings true for IoT [3].

(c) Dynamic Nature

The primary activity of Internet of Things is to collect data from its environment, this is achieved with the dynamic changes that take place around the devices. The state of these devices change dynamically, example sleeping and waking up, connected and/or disconnected as well as the context of devices including temperature, location and speed. In addition to the state of the device, the number of devices also changes dynamically with a person, place and time.

The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically [4].

(d) Enormous scale

The number of devices that need to be managed and that communicate with each other will be much larger than the devices connected to the current Internet. The management of data generated from these devices and their interpretation for application purposes becomes more critical. Gartner (2015) confirms the enormous scale of IoT in the estimated report where it stated that 5.5 million new things will get connected every day and 6.4 billion connected things will be in use worldwide in 2016, which is up by 30 percent from 2015. The report also forecasts that the number of connected devices will reach 20.8 billion by 2020.

The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.[2]

The Internet of Things can be considered as an intertwined system which is perfectly able to address physical component with many levels of processing, sensing, and actuation capabilities that be able to communicate via internet as joint platform [5]

RESEARCH CHALLENGES

'For all the above applications domains of Internet of things. Internet of things has many challenges must be sorted out for Internet Of things evolution. These challenges have two factors the metrics which they are heterogeneous technologies that are used in sensing, collection and sorting the date, with the second factor is all of that require more attention in different research areas [8]. On the other hand, many surveys of the Internet of things include a section of research challenges, so I have tried to consolidate their results here for our target. A. Privacy and data protection: The Internet of Things is known to be "an international network infrastructure, linking physical and virtual objects through the exploitation of information capture and communication capabilities. This infrastructure includes existing and involving web and network developments. it will provide specific objectidentification, sensing element and association capability because the basis for the event of freelance cooperative services and applications. These are going to be defined by a high degree of autonomous information capture, event transfer, network property and ability."

This ends up in a variety of new (as well as already known) potential risks regarding data security and each privacy and information protection, that should be thought about. The severity and probability of every risk can rely on the circumstances during which every IoT application / system is deployed.'[6]

While coming to the Things that can be any object or person which can be distinguishable by the real world. Everyday objects include not only electronic devices we encounter and use daily and technologically advanced products such as equipment and gadgets, but "things" that we do not do normally think of as electronic at all—such as food, clothing; and furniture; materials, parts and equipment, merchandise and specialized items; landmarks, monuments and works of art and all the miscellany of commerce, culture and sophistication [12].

SECURITY CHALLENGES FACING IOT

'IoT security is the protection of Internet of Things devices from attack. While many business owners are aware that they need to protect computers and phones with antivirus, the security risks related to IoT devices are less well known and their protection is too often neglected.

Internet of Things devices are everywhere. From cars and fridges to monitoring devices on assembly lines, objects around us are increasingly being connected to the internet. The speed at which the IoT market is growing is staggering - Juniper research estimates that the number of IoT sensors and devices is set to exceed 50 billion by 2022.While consumer IoT devices allow lifestyle benefits, businesses are quickly adopting IoT devices due to high potential for savings. For example, after Harley-Davidson turned their York, Pennsylvania plant to a 'smart factory' using IoT devices in every step of the production process, they reduced costs by 7% and increased net margin by 19%.

(a) Data Integrity

Billions of devices come under the umbrella of an interlinked ecosystem that is connected through IoT. Manipulating even a single data point will result in manipulation of the entire data which is exchanged and shared back and forth from the sensor to the main server. Decentralized distributed ledger and digital signatures should be implemented in order to ensure integrity [9].

(b) Encryption Capabilities

Data encryption and decryption is a continuous process. The IoT network's sensors still lack the capability to process. The brute force attempts can be prevented by firewalls and segregating the devices into separate networks.

Figure 3: Security Challenges Facing IoT[2]

(c) Privacy Issues

IoT is all about the exchange of data among various platforms, devices, and consumers. The smart devices gather data for a number of reasons, like, improving efficiency and experience, decision making, providing better service, etc.; thus, the end point of data shall be completely secured and safeguarded.

(d) Common Framework

There is an absence of a common framework and so all the manufacturers have to manage the security and retain the privacy on their own. Once a common standardized framework is implemented, the individual efforts will then collectively be utilized in an expandable manner and so reusability of code can be achieved [8].

(e) Automation

Eventually, enterprises will have to deal with more and more number of IoT devices. This enormous amount of user data can be difficult to manage. The fact cannot be denied that it requires a single error or trespassing a single algorithm to bring down the entire infrastructure of the data [7].

(f) Updations

Managing the update of millions of devices needs to be adhered to, respectively. Not all the devices support over the air update and hence it requires manually updating the devices. One will need to keep a track of the available updates and apply the same to all the varied devices. This process becomes time-consuming and complicated and if any mistake happens in the process than this shall lead to loopholes in the security later. Security Investment in securing infrastructure and network should be the first priority, which is not the case now. IoT involves the use of millions of data points and each point should be secured. Indeed, the need is for the multi-layer security, i.e., security at each and every level. From end-point devices, cloud platforms, embedded software to web and mobile applications that leverage IoT (Internet of Things), each layer should be security intact. With the set of heterogeneous devices, security becomes complex'.[2]

Disadvantages of IoT Applications

'Privacy issues: Hackers can break into the system and possibility of stealing the data.
Becoming Indolent: People are more habituated to have a click based work making them lazy to any sort of physical activity, applied science in their daily routine.
Unemployment: Lower level people like unskilled labour may have high risks of losing their jobs.'[11]

CONCLUSION

IoT has been considered to bring technological changes in our everyday life, which in helps to making our life simpler and comfortable. With various technologies and applications, there are many applications in IoT for the

Domains in medical, engineering, manufacturing, banking, development, infrastructure, industrial, transportation, education. Uses of IoT in various applications are discussed in this paper. In present and in future also, IoT is on the way of making the human's life easier and comfortable.

References:

1) Internet of Things (IoT), Radouan Ait Mouha , Anhui Polytechnic University, Wuhu, China, How to cite this paper: Mouha, R.A.(2021) Internet of Things (IoT). Journal of Data Analysis and Information Processing,9, 77-101.https://doi.org/10.4236/jdaip.2021.92006
2) Internet of Things (IoT) Applications and Security Challenges: A Review Mohit Kumar Saini1 1Department of Computer Application, Doon Business School, Dehradun Uttrakhand, India Rakesh Kumar Saini2 2Department of Computer Application, DIT University, Dehradun Uttrakhand, India..

3) M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.

4) S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective,"IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

5) M. Miraz, M. Ali, P. Excell, and R. Picking, "Internet of Nano-Things, Things and Everything: Future Growth Trends", Future Internet, vol. 10, no. 8, p. 68, 2018, DOI: 10.3390/fi10080068.

6) Research Challenges and Future Applications in Internet of Things Ahmed Aly, Riham Haggag, Informatics Bulletin, Faculty of Computers and Artificial Intelligence, Helwan University Published Online Vol 3 Issue 3, October2021 (https://fcihib.journals.ekb.eg)

7) C. Hong song, F. Zhongchuan, and Z. Dongyan, "Security and trust research in m2m system," in Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on. IEEE, 2011, pp. 286–290.

8) I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, "Trust in m2 communication," Vehicular Technology Magazine, IEEE, vol. 4,no. 3, pp. 69–75, 2009.

9) J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks.

10) Miao W., Ting L., Fei L., ling S., Hui D., 2010. Research on the architecture of Internet of things. IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), Sichuan province, China, Pages: 484-487.

11) A Review Paper on Internet of Things (IoT) and it's Applications Mrs. Sarika A. Korade1, Dr. Vinit Kotak2, Mrs. Asha Durafe3, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

12) Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. Advances in Internet of Things: Scientific Research, **1**, 5-12.
http://dx.doi.org/10.4236/ait.2011.11002