World Journal of Engineering Research and Technology

WJERT

www.wjert.org

Impact Factor Value: 5.924

A REVIEW OF THE INTERNET OF THINGS: APPLICATIONS, ARCHITECTURE, FUNCTIONING & SECURITY CONCERNS

Garv Pundir*

Vasant Valley School, Vasant Kunj, New Delhi, India.

Article Received on 25/02/2021 **Article Revised on 15/03/2021** **Article Accepted on 05/04/2021**

***Corresponding Author**
Garv Pundir
Vasant Valley School, Vasant Kunj, New Delhi, India.

ABSTRACT

During the recent past, IoT has emerged as a path- breaking technology which is acquiring a vast usage across the world. The study highlights the significance of IoT networks to industries including manufacturing, healthcare, logistics, farming and infrastructure. It discusses the IoT architecture and the technologies used by the IoT to function. However, the IoT is quite prone to privacy and security threats and vulnerabilities. The study discusses the definition of security with respect to IoT along with its associated challenges. The weaknesses and potential threats posed by these issues need to be addressed on priority. The study covers appropriate solutions such as Centralised Monitoring System and Software Defined Networking tools to curb these threats along with formal anticipation of threats to network weaknesses. These techniques will help to protect privacy and prevent potential damage. The study discusses the impact of these solutions in the effective utilisation of the IoT networks. The entire study has been conducted while keeping in mind the growing popularity and the projected growth in the usage of IoT networks in times to come.

KEYWORDS: IoT architecture, IoT applications, IoT security requirements, IoT threats and vulnerabilities, Security issues.

INTRODUCTION

According to www.wired.co.uk, the term IoT encompasses everything connected to the internet, but it is increasingly being used to define objects that "talk" to each other. "Simply, the Internet of Things is made up of devices – from simple sensors to smartphones and wearables – connected together," Matthew Evans, the IoT programme head at techUK says.[1]

The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data.[2] If we combine these connected devices with automated systems, it is possible to "gather information, analyse it and create an action" to help someone with a particular task, or learn from a process.[1] The information collected may pertain to man- made machines or humans themselves.

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.[3] From the smallest lightbulb to a driverless truck to smart homes and smart city projects, can all be part of the bigger Internet of things.

In Figure 1, IoT connected devices installed base worldwide from 2015 to 2025 (in billions) can been seen. It is evident that the growth (75.44 billion connected devices by 2025) has been projected in leaps and bounds.

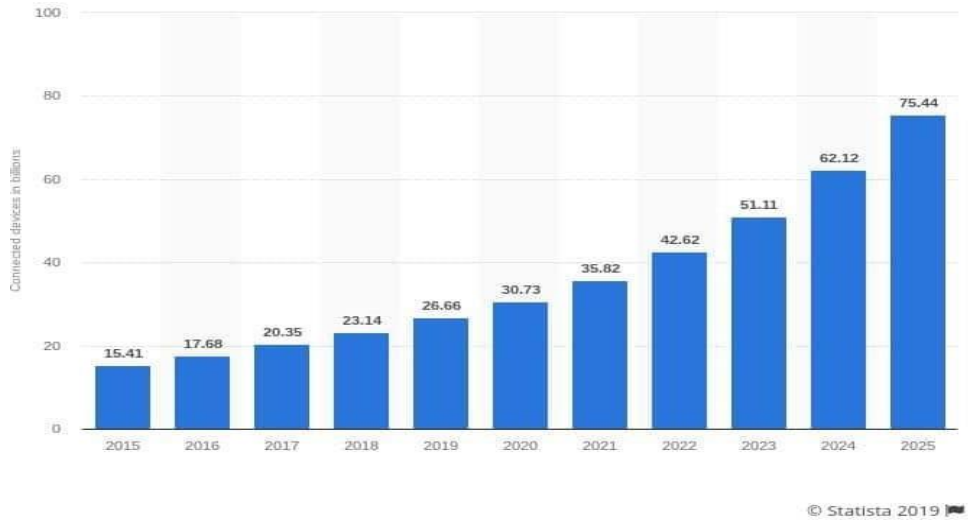

Figure 1: IoT connected devices installed base worldwide from 2015 to 2025 (in billions)

Source: Statista, 2019

HISTORY OF IoT

The Internet of Things is a technological revolution that represents the future of computing and communications, and its development depends on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology.[4] In 1982, a modified Coke machine at Carnegie Mellon University became the first connected smart appliance. Using the university's local ethernet or ARPANET – a precursor to today's internet – students could find

out which drinks were stocked, and whether they were cold.[5] Right from the beginning the Internet of Things evolution started, there were many things or objects connected to the internet for the different applications through diverse technologies depending on the type of object for the comfort ability of Human.[6]

APPLICATIONS OF IOT

The IoT revolution is having the capacities to make today's industries extra-effective, more-sustainable and cost-effective.[7] IoT has brought the whole world together as it has become utmost important in everyday life. People are better able to manage their lives and homes and gain the maximum by making use of this technology. Not just this, it is even more important for organisations.

IoT helps businesses by providing them insights about their systems and performance of various functions. Thus, it helps in feeding inputs to the process of decision- making regarding automation which further leads to reduction in costs. Consumer requirements and consumer psychology can also be better understood by making use of IoT. This helps them to serve the customers better, customise processes to suit the customer requirements, optimise their service delivery, quality, remove any glitches in operations and come up with smarter and newer ways to function and keep themselves technologically updated.

The benefits of IoT may apply to specific industries such as manufacturing, transportation and utility organizations, making use of sensors (used to monitor events or changes within structures). The other benefits may be applicable to organizations across multiple industries such as agriculture, infrastructure and home automation industries.

While H. Xu,[8] have conducted survey and found that IoT can enable global connectivity, also can bring in efficiency in sectors like healthcare visa-via logistics, therapy, diagnosis, recovery, management, medication, and finance.

According to Saini & Saini,[9] some useful applications of Internet of Things (IOT) are Smart Healthcare, Smart Cities, Connected Cars, Smart Homes, Smart Farming, Smart Retail, Smart Supply Chains. Smart Health/ Digital Health ranges from remote monitoring equipment to advance & smart sensors to equipment integration. IoT helps in revolutionizing healthcare and provides cost- effective and efficient solutions for the patient irrespective of their location. Also, companies like Nest, Ecobee, Ring and August are in the offing to render state-of-the-art

technology and become household brands for smart homes.

IOT ARCHITECTURE

According to Leloglu,[10] the IoT architecture has been proposed as follows:

1. Perception Layer: This is the first layer which identifies the unique objects and utilises sensor technology to collect all information pertaining to these objects. A number of other features such as nano technology and tagging technology are also present in the perception layer to support the main function of this layer.
2. Network Layer: This is the second layer which transfers the information collected fromthe unique objects via the sensors to the information processing unit. This layer is madeup of a number of wireless networks including Wireless Sensor Networks, communication networks such as 2G/3G, optical fibre, broadband and data networks.
3. Support Layer: This is the third layer which converts one form of information coming in into another form by means of the information processing unit. This processed information is sent to be stored by the centralised data unit. This can be retrieved by applications as and when a need arises.
4. Application Layer: This is the fourth and final layer which includes user specific applications, used to facilitate both individual and organisation specific requirements. This is the layer which helps realise the purpose of IoT in its real sense by facilitating industries as well as needs of individuals.

FUNCTIONING OF IOT

The IoT is a realm where physical items are consistently integrated to form an information network with the specific end goal of providing advanced and smart services to users.[11] The IoT system is enabled by the web technology. It includes smart devices such as processors, sensors and communication hardware. All these are combined to collate, transfer and process information received from these devices. The devices do most of the work without human intervention. Radio Frequency Identification (RFID) is a system that transmits the identity of an object or person wirelessly using radio waves in the form of a serial number.[6] In the IoT model, sensor-equipped devices know how to deliver lightweight data around the physical world, authorizing cloud-based resources to extract data and make choices from the extracted data by using actuator-equipped devices, which enhance the communication among nodes.[12] The following diagram explains this process.

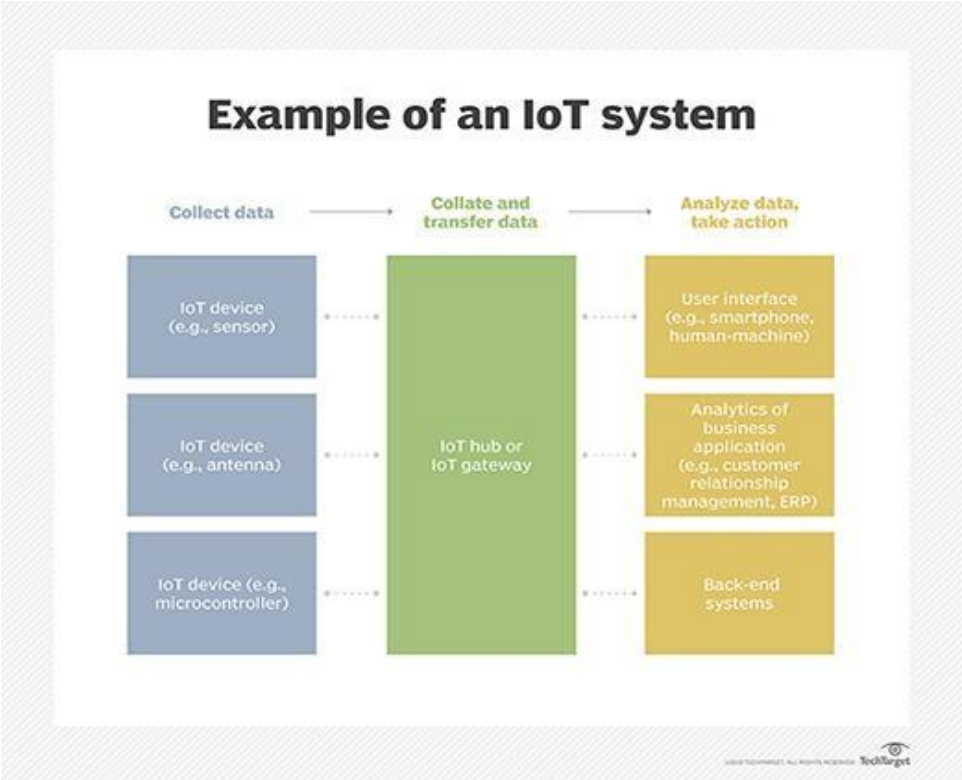

Figure 2: Functioning of IOT System.

Source: Techtarget.com

According to www.sas.com,[13] the following technologies play an important role in the functioning of IoT:

- **Data management and streaming analytics:** There is a lot of requirement for big data streaming from sensors involved in IoT. Every event is streamed to be filtered, standardised, correlated and analysed. It performs real-time data management and analytics on IoT data to make it more valuable.
- **Big data analytics:** Getting value from the massive volume, velocity and variety of structured and unstructured data businesses collect every day requires big data analytics. The techniques involved in this process are predictive analysis, text mining, cloud computing, data mining, data lakes and Hadoop or an optimum combination of these.
- **Artificial intelligence:** Artificial intelligence can enhance the value of IoT by makinguse of all the information from connected devices to promote the process of learning and collective intelligence. The techniques involved in this process are MachineLearning, deep learning and computer vision.

IOT SECURITY: DEFINITION, CONCERNS, CHALLENGES & SOLUTIONS

IOT security is concerned with safeguarding "things" in the Internet of things. IoT systems are prone to security attacks for a variety of reasons including the wireless communication between devices, physical access to objects, constrained capacity of smart devices and openness of thesystem.[14]

Shaikh, Mohiuddin & Manzoor,[24] have defined security in the scope of Internet of Things as per the **IAS-octave security requirements** as follows**:**

- Confidentiality(C): Ensuring that only authorized users access the information
- Integrity(I): Ensuring completeness, accuracy, and absence of unauthorized data manipulation
- Availability(A): Ensuring that all system services are available, when requested by an authorized user
- Accountability (AC): An ability of a system to hold users responsible for their actions
- Auditability (AU): An ability of a system to conduct persistent monitoring of all actions
- Trustworthiness (TW): An ability of a system to verify identity and establish trust in a third party
- Non-Repudiation (NR): An ability of a system to confirm occurrence/non-occurrence of an action
- Privacy (P): Ensuring that the system obeys privacy policies and enabling individuals to control their personal information.

IOT technology is faced with a lot of security concerns. IoT is accepted as an extended version of some different technologies such as Wireless Sensor Networks, Mobile Broadband and 2G/3G Communications Networks which are already under threat because of various security flaws.[10] There is a threat to privacy as objects in IoT share data with each other. It also opensup companies all over the world to more security threats, such as hacking.

There lie immense challenges in managing the entire data that objects are producing every minute. Companies need to figure out a way to store, track, analyse and make sense of the vast amounts of data that will be generated.[17] Efficient systems and implementation of techniques may bring some relief to this herculean task. It may also prevent any gaps from arising which may lead to potential damages to an organisation's systems and performance.

Attacks in IOT are possible as the devices in the IoT network are an easy target for

intrusion.[18] According to the report published by director of finance Kopetz in June 2017, IoT attacks have been carried out on half of US financial firms resulting in an approximate breach cost of $20 million for big companies.[19] The negative impact of these attacks may be manifold in terms of productivity and profits of these firms.

It is hence apparent that, in such a scenario, cybersecurity becomes critical to avoid threats like leakage of sensible information, denial of service (DoS) attacks, unauthorized network access, and so on.[20] Security issues, such as privacy, authorization, verification, access control, system configuration, information storage, and management, are the main challenges in an IoT environment.[21] Many devices like smartwatches and phones have provided path-breaking services to enable a global platform to operate and at the same time provide user- friendly interfaces. However, security remains a concern as users' privacy may be left unattended. To extensively adopt the IoT, this issue should be addressed to provide user confidence in terms of privacy and control of personal information.[22] Addressing these privacy concerns is utmost important to the development of IoT.

According to Abomhara & Koien,[22] all IoT devices and services are exposed to a number of common threats and vulnerabilities like viruses, physical attacks, privacy attacks and denial-of-service attacks. One needs to conduct an in- depth study of the system assets such as hardware, software, data and services assets such as service branding. This should be followed by a deep understanding of the possible threats and vulnerabilities. A careful mapping should be done so as to understand which of these threats and vulnerabilities have already been protected by the Cyber Security. Additionally, potential threats and vulnerabilities need to be anticipated to work in the direction of optimum system development and effective fund allocation. The process of policy implementation needs to follow stringent measures. The various threats have been classified as individual attacks, organized groups, and intelligence agencies. Each of these may vary in their motivation to attack, level of skills, resources and ability to tolerate risk. By studying and collating all this information, a prediction can be made about a possible threat exploiting a vulnerability in the system. Therefore, the IoT architecture must be designed so as to accommodate these weak devices and at the same time be efficient in identifying such occurrences. Thus, it can be found that a careful study of the attackers' tools and techniques is utmost important to protect the system's vulnerabilities from a possible attack. Discrete research may support to enhance knowledge and timely awareness about these attacks. Thus, potential damage can be prevented.

According to Shaikh, Mohiuddin & Manzoor.[24] IoT has made immense progress in the direction of technology standardization. However, security and privacy are very crucial to protect IoT systems. Possible areas for attacks can be identified by studying the current problems. These can provide useful insights to make major improvements during the development. Fixing these problems with effective solutions during the production phase may help develop a full- proof system. Improvised security frameworks can tackle security issues at a wider and deeper scale. In order to facilitate these security mechanisms; individuals, organisations, planners and developers should work hand-in-hand to propose a secured IoT environment. Also, misuse of data can be prevented by sharing only the required information at the required time. This would enable a faster and efficient process which is safe from privacy attacks.

According to Hameed, Khan & Hameed,[25] privacy provisioning, lightweight cryptographic framework, secure routing and forwarding, robustness and resilience management, denial of service, and insider attack detection can ensure security in the IoT network. Also, lightweight cryptographic primitives have been proposed to be most suitable for securing IoT networks. Additionally, context-aware techniques and lightweight protocols for privacy and virtualization techniques for maintaining the integrity of the data. Software Defined Networking (SDN) techniques may be used to execute lightweight cryptographic solutions over IoT along with centralized routing carried at the SDN controller. Network attacks may impose IoT network failures. These may be an outcome of denial-of-service attacks or frequent insider attack within the IoT network. Centralized monitoring of the network can help to curb these faults. SDN can support centralized monitoring of the network by routing to alternative servers or pathways in order to enable efficiently functioning IoT network. Moreover, this can help in identifying DDoS and diminish their effects within the IoT network. Therefore, SDN can help to deal with the different privacy and security issues through a centralised monitoring system. However, further insights into SDN can help in tailor- making it to provide management services over IoT network.

A lot is being done to curb the challenges posed by the ever-growing use of the Internet of Things. Physical attacks, Denial- of- Services, viruses and privacy attacks are possible due to the inherent nature of this technology. It is so because so much data is being transferred amongst devices which use embedded technology. Not only this, people and entities involved in Cyber crime are also responsible for these threats which exploits each vulnerability of these

networks. Careful and robust planning combined with timely action may help prevent these threats as well as fix the existing issues and concerns.

CONCLUSION

Today, we're living in a world where there are more IoT connected devices than humans. The real-time insights gleaned from this IoT collected data fuel digital transformation. IoT promises many positive changes for health and safety, business operations, industrial performance, and global environmental and humanitarian issues.[5] IoT is making the fabric of the world around us smarter and more responsive, merging the digital and physical universes. Threats and vulnerabilities to IoT network need to be carefully anticipated and evaluated in order to prevent potential destruction from occurring. One option is to design the IoT architecture in a way as to discourage these security and privacy- related incidents to occur. Another good option is to identify these problems during the development, so as to work around their solutions in the production. SDN has been recommended to enable centralised monitoring system and has the capacity to deal with privacy and security threats. However, there are issues involving in- depth study and application of the virtualisation technology/SDN system to further address these concerns.

REFERENCES

1. What is the Internet of Things? WIRED explains | WIRED UK.
2. What is the IoT? Everything you need to know about the Internet of Things right now | ZDNet.
3. What is IoT (Internet of Things) and How Does it Work? (techtarget.com).
4. http://www.ieccr.net/comsoc/ijcis/.
5. The Internet of Things (IoT) - What it is and why it matters | SAS India.
6. Internet of Things (IoT): A Literature Review (scirp.org).
7. Pandow B.A., Bamhdi A.M. and Masoodi F. Internet of Things: Financial Perspective and Associated Security Concerns. *International Journal of Computer Theory and Engineering,* 2020; 12(5): 123-127.
8. H. Xu, "Internet of things in industries: A survey*," IEEE Transactions on industrial informatics,* 2014; 10(4): 2233-2243.
9. Saini M.K. and Saini R.K. Internet of Things (IoT) Applications and Security Challenges: A Review. *International Journal of Engineering Research & Technology (IJERT)* ISSN: 2278-0181, 2019; 7(12): 1-7. Published by www.ijert.org NCRIETS – 2019 Conference

Proceedings.

10. Leloglu, E. A Review of Security Concerns in Internet of Things. *Journal of Computer and Communications,* 2017; 5: 121-136. doi: 10.4236/jcc.2017.51010.
11. Botta A., Donato W., Persico V., and Pescapé A. Integration of Cloud Computing and Internet of Things: A Survey. *Future General Computer Systems*, 2016; 56: 684-700.
12. Borgia, E., Gomes, D. G., Lagesse, B., Lea, R., and Puccinelli, D. Special issue on "Internet of Things: Research challenges and Solutions, 2016; 90: 1–4.
13. www.sas.com.
14. S. Sicari et al., "Security, privacy and trust in Internet of Things: The road ahead, *Computer Networks*, 2015; 76: 146-164.
15. Shaikh E., Mohiuddin I. and Manzoor A. Internet of Things (IoT): Security and Privacy Threats. 978-1-7281-0108-8/19 IEEE. DOI: 10.1109/CAIS.2019.8769539, 2019.
16. Gupta, J., Nayyar, A. and Gupta, P. Security and Privacy Issues in Internet of Things(IoT). *International Journal of Research in Computer Science*, 2015; 2: 18-22.
17. A Simple Explanation Of 'The Internet Of Things' (forbes.com).
18. X. Xiaohui, "Study on security problems and key technologies of the internet of things," in Proceedings of *IEEE Fifth International Conference Computational and Information Sciences(ICCIS)*, Hubei, China, June 2013.
19. H. Kopetz, "Internet of things," *in Real-Time Systems*, Boston, MA. Springer, 2011; 307-323.
20. https://www.sciencedirect.com/science/article/pii/.
21. Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu Security of the Internet of Things: perspectives and challenges. *Wireless Networking*, 2014; 20(8): 2481-2501.
22. Li S., Tryfonas T., and Li H. The internet of things: A Security Point of View. *Internet Research*, 2016; 26(2): 337-359.
23. Abomhara M. and Koien G. M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security,* 2015; 4: 65–88. doi:10.13052/jcsm2245-1439.414.
24. Shaikh E., Mohiuddin I. and Manzoor A. Internet of Things (IoT): Security and Privacy Threats. 978-1-7281-0108-8/19 IEEE. DOI: 10.1109/CAIS.2019.8769539, 2019**.**
25. Hameed S., Khan F. I., and Hameed B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *Hindawi Journal of Computer Networks and Communications,* 2019. Article ID 9629381, 14 pages https://doi.org/10.1155/2019/9629381.

26. www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.
27. A. Mosenia and N.K. Jha, (September). “A comprehensive study of Internet ofThings.” In Emerging Topics in Computing. [Online], 2016; 5(4): 586-602. Available: https://ieeexplore.ieee.org/document/7562568.
28. Alaba F.A., Othman M., Hashem I.A.T., and Alotaibi F. Internet of Things security: A survey. *Journal of Network and Computer Applications*, 2017; 88: 10-28. https://doi.org/10.1016/j.jnca.2017.04.002.
29. F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in *IEEE Internetof Things Journal*, 2019; 6(5): 8182-8201, doi: 10.1109/JIOT.2019.2935189.
30. Yan, P. Zhang and A.V. Vasilakos A survey on trust management for Internetof Things. *Journal of Networking and Computer Applications*, 2014; 42: 120-134.