WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on IOT Technology and Its Applications

Mihir Suresh Gadhiya[1], Nihal B. Jiwane[2], Ashish B. Deharkar[3]

Student, Computer Science & Engineering , Shri Sai College of Engineering and Technology, Bhadrawati, India[1]

Assistant Professor, Computer Science & Engineering , Shri Sai College of Engineering and Technology , Bhadrawati, India[2]

Assistant Professor, Computer Science & Engineering , Shri Sai College of Engineering and Technology , Bhadrawati, India[3]

ABSTRACT:

Internet of things (IoT) could be a terribly distinctive platform that is obtaining extremely popular day by day. The terribly reason for this to happen is that the advancement in technology and its ability to get connected to everything. This feature of obtaining connected has in itself provided multiple opportunities and an enormous scope of development. the very fact that technology in numerous fields has evolved through the years, is that the reason why we tend to observe a speedy amendment within the form, size and capability of assorted instruments, parts and also the product employed in way of life. And this benefit of simplified technology once amid a platform like IoT eases the work in addition as benefits each the manufacturer and also the user. the net of Things gives North American country a chance to construct effective administrations, applications for manufacturing, delivery solutions, correct cultivation and a lot of. This paper proposes an intensive overview of the IoT technology and its varied applications in life saving, sensible cities, agricultural, industrial etc. by reviewing the recent analysis works and its connected technologies. It additionally accounts the comparison of IoT with M2M, points out some disadvantages of IoT. Furthermore, an in depth exploration of the present protocols and security problems that might enable such applications is elaborate. Potential future analysis directions, open areas and challenges featured within the IoT framework are summarized.

Keywords: Internet of Things (IoT), IoT security , Wireless Sensor, Security, IoT applications, distributed systems.

1.Introduction

IoT could be a dynamic network framework that intends to coalesce the physical and therefore the virtual domains by utilizing the net because the medium for communication and transmission of data between them. Physical and virtual worlds square measure dead amalgamated into one huge data network with the usage of communication protocols within the self-configuring IoT infrastructure. it's been characterised as an appointment of reticular computing gadgets, mechanical and electronic machines, articles, creatures or people that square measure stocked with one amongst a form identifiers and therefore the ability to exchange info over a system while not requiring human -human or human–machine interaction[1]. IoT could be a returning elderly revolution affecting various lives worldwide that aims at autonomously operational devices without human intervention whereas establishing the machine to machine (M2M) communication. The interconnection of objects at anytime, anywhere for all the world by usage of any sensible network has continuously been the vision of IoT.

The label “Internet of Things” was developed in 1999 by Kevin Sir Frederick Ashton and since then this omnipresent property network has sealed its manner into our daily lives and have been vividly utilized in planet applications like defence, medicine, industry, agriculture, energy and for the creating of sensible cities, homes and devices. With the utilization of net and artificial intelligence it's creating our world smarter whereas minimizing the manual efforts and being a lot of and a lot of human-friendly. the elemental plan of associate degree IoT system is the trade of information between machines that square measure evoked by leading edge technologies like WSN (Wireless device Networks) and RFID (Radio Frequency Identification) with usage of sensing devices with effective higher cognitive process skills and intelligent algorithms when which associate degree action is performed consequently. IoT systems square measure deployed with success by enabling telecommunication interfaces with the net in devices like sensors and actuators with storage and process sections for eminent interactions between machines. With the comfort it offers, this new paradigm conjointly comes with some privacy and security problems which has to be rectified for its correct utilization and functioning. the net of Things (IoT) forms a process concept portrays a future wherever regular physical things will be related to the net and are capable to acknowledge themselves to different devices[2].

RFID that was frst introduced in 1945 could be a necessity of IoT. it's a programmed innovation that helps machines and digital devices to acknowledge objects, record information and management singular target through radio waves [4]. Normally, a RFID framework comprises of tags and readers. The tag could be a semiconductor device related to a receiving wire, which can be connected to any object as a novel identifier. With the employment of radio waves, there's a part of communication between the RFID's reader and its tag that helps within the autonomous identification and classification of the thing. aside from RFID, there area unit varied forms of technologies employed in IoT like WSN, Electronic Product Code (EPC), Bar Code, ZigBee similarly as Bluetooth that uses low energy supply and its one of the foremost convenient and in style IoT sanctioning technology. Currently, there area unit regarding twenty five billion devices interconnected by the IoT which might ragingly grow to regarding sixty billion by the year 2025[3].

IoT forms a cyclic development which mixes the usage of sensors to make a connection and sense the user and a network to speak with an individual because it additional aggregates the standards and provides a machine with increased intelligence that helps it to analyse, behave and act in keeping with matters. The action, creation, communication, aggregation and therefore the Analysis of a tool square measure the combined functions that makes it interconnected to IoT by establishing an increased intelligence for it and creating it a wise device. This IoT method operates in an exceedingly cycle with everything dependent on each other for its prospering execution. transient IoT Constituents parts square measure[5].

2.Technology Used In IOT

In IoT applications, it's necessary to transmit the info generated by the devices or sources to the web. Proving property and coverage could be a intimidating task for IoT applications. The users or vendors perpetually wished to gather knowledge and analyse it for any process for better sweetening of their devices. it's necessary to properly advent new technologies for act and process the info. instead of aiming to different network, a better privileged network particularly for its own applications would be an honest selection[6]. Nowadays, the industries ar actively concerned developing wired or wireless communication channels or protocols. however the price and infrastructure development plays a significant role in developing technology for IoT.

WIRELESS SENSOR-

The advancement of wireless detector networks (WSN) was galvanized by military applications, today, they comprise of condemned free gadgets that utilizes the detector to screen the physical conditions with their applications stretched to the economic infrastructure, robotization, wellbeing, activity, and diverse client regions. Wireless detector network is part of the IoT category. Reconfigurable uniform or heterogeneous network eventualities like automatic network management is that the would like of the hour for IoT.

For IoT and wireless detector networks short vary communication Bluetooth is most preferred. this is often one in all the effective wireless technologies that permits to the transfer the data during a short vary around 10–100 m, between devices like mobiles, PCs, cameras etc. and usually the communication speed is a smaller amount than one Mbps. In 1994 one mobile communication company fabricated this Bluetooth. it had been created for private space network, and later piconet was fabricated that was a group of 2–8 Bluetooth devices. once it involves the enhancement of the options of wireless detector network and IoT, the protocol that was created was named as ZigBee. it had been based within the year 2001. ZigBee features a flexible protocol style and is employed briefly transmission ranges. ZigBee covers the space of one hundred and a information measure of 250 kbps[7].

CHALLENGES OF IOT-

;As the principle of IoT involves connecting devices, it makes everything available and locatable that successively makes our life easier. However, creating everything connected to net opens the door for hackers. while not correct confidence concerning privacy and security, user won't be attracted towards IoT [3]. So, it should have a robust infrastructure dealing with security and a few of the problems that IoT would possibly face square measure listed below. The primary issue the IoT facing is unauthorized Access to RFID. The RFID tags will contain any form of data and as RFID tag is simply modified or browse by the reader[8]. This opens a full bunch of threat for the user because the knowledge is simply accessed by a wrongdoer reader.. Wireless device networks security breach sensors node in IoT are bifacial. Acquisition of information is additionally attainable aside from transmission. during this scenario, a number of the attainable attacks embody change of state wherever the info within the node is extracted or altered. Next fooding creates a full ton of issues in IoT.

Flooding the name suggests, it explains once traffic quantity is high and exhaustion of memory takes place. Sybil attack whereby multiple pseudo identities square measure claimed for a node order for it to present massive influence. Security problems from robot wherever once once we connect IoT to associate robot, not like IOS robot it's associate open supply network which implies it will simply be discovered. Once the front devices square measure compromised, the IoT network is exposed. computer code change downside is typically sweet-faced by the developers thanks to high cost and memory, they are doing not update their computer code and devices. Once the hackers discover the devices, they'll be simply accessed. Cloud Computing in IoT could be a massive network that allows sharing of resources and a few of the protection threats sweet-faced by shared resources square measure listed below[9]. Data loss happens once any wrongdoer user having unauthorized access will modify or delete the info. Cloud

computing may also be used for dominant different devices, once the hackers come up of associate account it will transfer bound software's which is able to offer him management of any devices that are available in contact.

SECURITY -

We see loads of reports reading regarding the those who suffered in emergencies condition what if somebody notify you before it truly happened, won't it's nice? Well IoT can play the role of that somebody in coming back years. Here we tend to discuss a number of its application in securities and emergencies[10]. Perimeter Access management detects and controls the individuals activity within an unauthorized ANd restricted space. Radiation Levels area unit usually employed in atomic energy plants or station to watch the extent of radiation so as to advise as before long as there's a leakage within the plant. Explosive and dangerous Gases detects the extent of gas during a chemical business and advise as before long as a escape is detected. Earthquake individuals suffer a loss of life ANd cash once an earthquake hits, the system will not save your cash however it can save your life, it notifies as before long because it detects the presence of earthquake and guides you the safest and fastest thanks to exit. Definitely IoT plays a significant role in dominant these applications[11,12].

DISADVANTAGE--

Though IoT has an oversized scope in most areas of our day to day applications. There area unit some disadvantages that hinders more implementation of the IoT systems at a quicker pace. the net of things makes the physical objects within the real setting to be seen in cyber globe and offers the formation of good systems and applications[13,14]. Networks of sensors, middlewares, electronic communication and computing, protocols etc. light-emitting diode to growth of interconnected devices. The advancement in communication, connection and integration helps to possess ton of selections to decide on devices and services. The variety of services and devices that gives similar functions cause search and discovery. the invention and categorization of comparable devices and services causes the system to become a lot of costlier and error prone. Addressing the disadvantages can allow next generation IoT to acknowledge and satisfy the data wants[15].

Conclusion

In this review, the technological normal needed for implementation of IoT is discussed. Moreover, basic communication entities and networks that support IoT also reviewed in such how to forsee the issues of ideal implementation of IoT.

REFERENCES

[1]. 1. Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefts and challenges. IEEE Internet of Things Journal, 5, 3758–3773.

[2]. Porkodi, R., & Bhuvaneswari, V. (2014). The Internet of Things (IoT) applications and communication enabling technology standards: An overview. In 2014 International conference on intelligent computing applications (ICICA), IEEE, pp. 324–329.

[3]. . Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.

[4]. Alam, M. M., Malik, H., Khan, M. I., Pardy, T., Kuusik, A., & Le Moullec, Y. (2018). A survey on the roles of communication technologies in IoT-based personalized healthcare applications. IEEE Access, 6, 36611–36631.

[5]. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376.

[6]. Singh, N., Bhatt, J., & Purohit, K. C. (2017). A survey on IoT and security issues of RFID. International Journal of Engineering and Computer Science, 6(4), 21061–21066.

[7]. European conference on antennas and propagation (EuCAP), IEEE, pp. 3638–3639. 13. Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014). A state of the art review on the Internet of Things (IoT) history, technology and felds of deployment. In 2014 International conference on science engineering and management research (ICSEMR), IEEE, pp. 1–8.

[8]. . Kazmi, A., Jan, Z., Zappa, A., & Serrano, M. (2016). Overcoming the heterogeneity in the internet of things for smart cities. In International workshop on interoperability and open-source solutions, Springer, Cham, pp. 20–35.

[9]. . Kubo. (2014). The research of IoT based on RFID technology. In 2014 7th international conference on intelligent computation technology and automation, Changsha, pp. 832–835.

[10]. . Khalid, A. (2016). Internet of Thing architecture and research agenda. Computer Science and Mobile Computing, 5(3), 351–356Dalkiltc, 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.

[11]. Naik, N. (2017). Choice of efective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In 2017 IEEE international systems engineering symposium (ISSE), IEEE, pp. 1–7. 21. 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.

[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]. . 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.

[14]. Kaedi, S., Doostari, M. A., & Ghaznavi-Ghoushchi, M. B. (2018). Low-complexity and diferential power analysis (DPA)-resistant two-folded power-aware Rivest–Shamir–Adleman (RSA) security schema implementation for IoT-connected devices. IET Computers and Digital Techniques, 12(6), 279–288.

[15]. Luoto, A., & Systä, K. (2018). Fighting network restrictions of request-response pattern with MQTT. IET Software, 12, 410–417.