IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CURRENT INTERNET OF THINGS: A MODERNITY

[1] Dr. Vaidya Krishna, [2] Kavish Samir Padshah
[1] Assistant Professor, [2] Grade 12 Student
[1]BCA Department,
[1] SDJ International College, Surat, India

Abstract: In the modern, technologically advanced world, the Internet of Things (IoT) has gained popularity. a robust cloud computing architecture, supported by a seamless integration of sensors and This "network of networks of autonomous objects" is becoming a reality thanks to actuators working with the environment around us. The Internet of Things is growing in a variety of sectors, including smart wearables, smart cities, home life, and business. By 2020, the Internet of Things will have 26 billion deployed devices, predicts Gartner Inc. In-demand IoT applications include smart security solutions, smart home automation, smart health care, smart wearables, etc. In the near future, we anticipate seeing IoT applications in smart power grids and municipal transportation systems. In addition to discussing the effects of the IoT on our daily lives, this paper provides a brief review of various IoT developments. As well in the context of the IoT, addresses the significance of cloud computing, autonomous control, and artificial intelligence. In order to properly use IoT enabling technologies, the Internet, wireless sensors and actuators, and distributed computing must be coordinated.

***Index Terms* - Smart Devices , Wireless Network, The Internet of Things, Cloud Computing, Embedded Systems, Machine Learning, Automation**

I. INTRODUCTION

A network of networks of physical objects, such as vehicles, buildings, machinery used in construction, and medical devices, make up the Internet of Things (IoT). Observation tools. Such a network would use electrical components like sensors and actuators to achieve its goals: information interchange and updating in order to reach agreement on the system's overall performance.
The idea of networked smart gadgets dates back to 1982, when a modified Coca-Cola machine at Carnegie Mellon University served as the first Internet device.

linked appliance [1] that can disclose its inventory and the temperature of recently filled drinks. Peter T. Lewis first used the phrase "Internet of Things" in 1985 during a speech at a wireless session sponsored by the Congressional Black Caucus' 15th Legislative Weekend Conference in the United States. "The Internet of Things, or IoT," he said in his lecture, "is the integration of people, processes, and technology with connectable devices and sensors to enable remote monitoring, status, manipulation, and evaluation of trends of such devices". The Computer of the 21st Century, a 1991 landmark study by Mark Weiser on ubiquitous computing, as well as academic forums like UbiComp and PerCom developed the modern vision of IoT.[2] [3].
With the help of MIT's Auto-ID Centre, the Internet of Things gained popularity in 1999 [4]. In order for computers to manage and inventory everyday objects, Kevin Ashton, one of the Auto-ID Center's founders, used to view radio-frequency identification (RFID) as a necessary component of the Internet of Things [5] [6] . Barcodes, QR codes, and Near Field Communication (NFC) technologies can also be used to tag items in addition to RFID [7].
The vision of IoT has significantly changed as of 2016. Numerous technologies, including cloud computing, wireless networking, real-time analytics, machine learning, sensors, and embedded systems, have come together [8]. The IoT is enabled by the conventional domains of embedded systems, wireless sensor networks, control systems, automation, and others [9].

II. TRENDS

A. Market Size

By 2020, 26 billion Internet of Things (IoT) devices are expected to be installed, according to Gartner's prediction [10]. At that point, IoT product and service providers are expected to earn additional income surpassing $300 billion, primarily from services.

Naturally, companies across all industries anticipate opportunities from IoT. Cisco Systems uses "the Internet of Everything" to define a combination of IoT and more conventional IT hardware (PCs, tablets, cellphones, etc.). According to Cisco, by 2015 there will be more mobile devices and smartphones linked than there are people on the entire planet. According to Cisco's predictions, 50 billion things and more than 5 billion people will be online by 2020 [8].

Large corporations view IoT prospects from many perspectives. The global network that links people, data, and machines is known as the "Industrial Internet," according to GE, for example. Additionally, according to CEO Jeff Immelt, the Industrial Internet could increase the GDP (global product) by $10 trillion to $15 trillion between 2012 and 2032. To develop relevant Industrial Internet technology and applications, GE is investing $1 billion.

B. Standards

Vendors and customers must adopt open standards that enhance device administration and monitoring, big data information collecting and analytics, and general network connections if IoT is to truly take off. The IEEE Standards Association (IEEE-SA) is working on important IoT standards efforts.

Additionally, vendor-led organisations are leading open source initiatives to expand IoT beyond the connected home, such as the AllSeen Alliance. Consumer electronics manufacturers, auto manufacturers, cloud service providers, retailers, software developers, and more make up the more than 100 member companies.

C. Security

According to Gartner [11], the proliferation of devices placed throughout various modern urban environments and their increasing digitalization and automation will pose new security issues to numerous sectors.

D. People and Process

Big data generated as a result of the deployment of numerous devices will significantly increase security complexity, meaning that significant security concerns will still exist. According to Gartner [11], this will have an effect on availability needs, which are also anticipated to rise, endangering real-time corporate operations and maybe personal safety.

E. Consumer Privacy

There will be a tremendous amount of data providing information on users' personal use of gadgets that, if not secured, can result in privacy breaches, much as is now the case with smart metering equipment and more digitalized autos. This is particularly difficult because, according to Gartner [11], the information produced by IoT is essential for improving services and managing such devices.

F. Data Management

When it comes to the types of data that need to be saved, the Internet of Things has a two-pronged impact: large data (driven by businesses) and personal data (driven by consumers). Significant data will be produced as apps and devices continue to learn about the user, according to Gartner [12].

G. Storage Management

As this data becomes more common, it will be necessary to address the impact of the IoT on storage infrastructure, which is another reason driving up the demand for more storage space. According to Gartner [11], the emphasis today must be on storage capacity as well as whether or not the organisation can gather and utilise IoT data in a cost-effective manner.

H. Server Investment

According to Gartner [11], the influence of IoT on the server industry will mostly centre on increased investment in important vertical sectors and businesses associated with those industries where IoT can be profitable or contribute considerable value.

I. Bandwidth

Current data centre WAN connections are sized to accommodate the moderate bandwidth demands brought on by user interactions with applications. According to Gartner [11], the Internet of Things (IoT) is expected to significantly alter these patterns by delivering enormous amounts of short message sensor data to the data centre for processing.

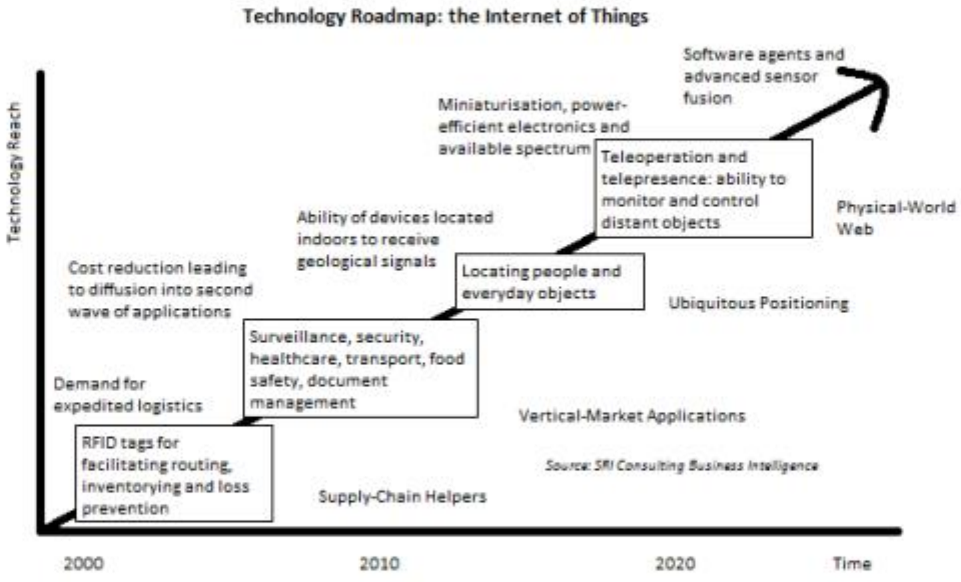

Fig. 1. Technology Roadmap : The Internet of Things

III. IOT ENABLING TECHNOLOGIES

The IoT is made possible by a variety of technologies. A number of wireless or wired networks can be used to establish connections between the various nodes of an IoT installation, which is their primary function.

- Radio Frequency Identification (RFID) was the dominant technology in the 2000s. Near Field Communication (NFC) eventually took the lead, though. During the 2010s, it became widely employed in smart phone technologies, either for reading NFC tags or for accessing various items like automated doors, merchant payment, etc.
- The IoT can benefit from advancements in optical technologies like Li-Fi (Light Fidelity) or Cisco's 40 Gbps bidirectional Internet.
- Using quick response (QR) codes allows for inexpensive tagging. Image processing is used to read QR codes using phone cameras.
- Due to its properties including low power consumption, low data rate, low cost, and fast message throughput, ZigBee communication technology, based on IEEE 802.15.4 2.4-GHz radio protocol, is expected to be an intriguing IoT enablement technology.
- IoT connectivity through twisted pair or fibre network cables is possible using Ethernet.
- Long Term Evolution's original LTE (Long Term Evolution) has been upgraded to LTE-Advanced, which has more coverage, higher throughput, and lower latency.
  It can be used for vehicle-to-vehicle (V2V) communication even though it is intended for mobile communications.
- WiFi-Direct, a wireless connection for peer-to-peer communication without a need for an access point, enables the development of Internet of Things (IoT) applications with lower latency and WiFi speed.
- Z-Wave is the most popular communication standard for smart home products. It employs a 900 MHz radio protocol. Z-Wave offers an easy and dependable approach to wirelessly manage lighting, HVAC (Heating, Ventilation, and Air Conditioning), security systems, etc. It is primarily geared at the domestic control and automation industry. A Z-Wave gateway or central control device can be used to control a Z-Wave automation system through the Internet while also acting as a portal to the outside world [13].
- IoT networking protocol called Thread is based on IPv6. Thread makes use of 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks), which in turn makes use of the mesh IEEE 802.15.4 wireless technology. On the other hand, thread is IPaddressable, offers cloud access, and can currently support up to 250 devices in a single local network mesh [14].

IV. LIMITATIONS

A. Cost of Implementation

Its implementation is achievable on a brand-new system that is now being built. However, it would need to be completely disassembled into pieces small enough to accommodate the installation of a network in order to be applied to an existing system. For instance, it would be impractical and expensive to disassemble and reassemble a home that already had fully functional water, electricity, cable television connections, and security systems.

B. Security and Privacy

As such a system would inevitably be vulnerable to hacking, it would also require perfect cyber protection. A power grid in western Ukraine was taken down by hackers in 2015 to launch the first cyber-attack-related blackout [15]. Less than 10,000 households can produce 150 million discrete data points per day, according to a Federal Trade Commission (FTC) report. This increases the number of hacker entry points and exposes private data to risk.

C. Network Space

Each device connected to the Internet will receive a special IP address. However, because IPv4 address spaces are running out, IoT items must use IPv6 in order to accommodate the incredibly enormous address space used. Since many ISPs have not yet adopted IPv6, the widespread usage of IoT-enabled technologies is constrained.

V. CONCLUSION

Here, we've concentrated on recent advancements and ongoing research in the IoT space. Other fields besides those already listed will also profit from it. Various governments are also supporting various IoT-based projects. Investment in IoT initiatives has already started in large sectors. The enabling technologies assist us in realising IoT systems and solutions before they are ready for widespread use, as was said in section III. By 2025, it is anticipated that the Internet of Things would be used in smart grids and cities. However, as indicated in section IV, IoT applications include security flaws much as other technological developments. When deploying IoT solutions, such should be taken into consideration. The FTC has already made a number of suggestions regarding data consent, data security, and data reduction. The IoT sector is actually developing a number of standards related to autos because the majority of issues with linked cars also apply to medical equipment.

REFERENCES

[1] C.-Z.-E. Li and Z. W. Deng, “The Embedded Modules Solution of Household Internet of Things System and The Future Development,” *Procedia Comput. Sci.*, vol. 166, pp. 350–356, 2020, doi: 10.1016/j.procs.2020.02.086.

[2] F. Mattern and C. Floerkemeier, “From the Internet of Computers to the Internet of Things,” in *From Active Data Management to Event-Based Systems and More*, K. Sachs, I. Petrov, and P. Guerrero, Eds., in Lecture Notes in Computer Science, vol. 6462. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 242–259. doi: 10.1007/978-3-642-17226-7_15.

[3] M. Weiser, “The Computer for the 21 st Century,” *Sci. Am.*, vol. 265, no. 3, pp. 94–105, 1991.

[4] D. K. Verma, U. Salman, and V. Samant, “An Application Perspective of IoT,” vol. 8, no. 2.

[5] L. Mirtskhulava, L. Tvaliashvili, A. Bardavelidze, and L. Tvaliashvili, “Environmental Monitoring in Flammable Climate Zones over IoT Cloud,” *Int. J. Simul. Syst. Sci. Technol.*, Mar. 2020, doi: 10.5013/IJSSST.a.21.02.34.

[6] A. Misbah and A. Ettalbi, “Towards Machine Learning Models as a Key Mean to Train and Optimize Multi-view Web Services Proxy Security Layer,” *Int. J. Recent Contrib. Eng. Sci. IT IJES*, vol. 6, no. 4, p. 65, Dec. 2018, doi: 10.3991/ijes.v6i4.9883.

[7] N. Letting and J. Mwikya, “Internet of Things (IoT) and quality of higher education in Kenya; A literature review”.

[8] S. Selvakumari, V. Vaneeswari, and S. Ranichandra, “INTERNET OF EVERYTHING”.

[9] T. Dutta, S. Pramanik, and P. Kumar, “IoT for healthcare industries: a tale of revolution,” in *Healthcare Paradigms in the Internet of Things Ecosystem*, Elsevier, 2021, pp. 21–45. doi: 10.1016/B978-0-12-819664-9.00002-8.

[10] Q. Ren, K. L. Man, M. Li, and B. Gao, “Using Blockchain to Enhance and Optimize IoT-based Intelligent Traffic System,” in *2019 International Conference on Platform Technology and Service (PlatCon)*, Jeju, Korea (South): IEEE, Jan. 2019, pp. 1–4. doi: 10.1109/PlatCon.2019.8669412.

[11] A. E. Oke, V. A. Arowoiya, and O. T. Akomolafe, “Influence of the Internet of Things’ application on construction project performance,” *Int. J. Constr. Manag.*, vol. 22, no. 13, pp. 2517–2527, Oct. 2022, doi: 10.1080/15623599.2020.1807731.

[12] M. Kajba and B. Jereb, “SUPPLY CHAIN IT TRENDS THAT HAVE BEEN SHAPING OUR TOMORROW,” 2021.

[13] C. Chakraborty, J. C.-W. Lin, and M. Alazab, Eds., *Data-Driven Mining, Learning and Analytics for Secured Smart Cities: Trends and Advances*. in Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-72139-8.

[14] Q. Zhou, L. Li, L. Wang, J. Xue, and X. Feng, “May-happen-in-parallel analysis with static vector clocks,” in *Proceedings of the 2018 International Symposium on Code Generation and Optimization*, Vienna Austria: ACM, Feb. 2018, pp. 228–240. doi: 10.1145/3168813.

[15] M. C. Libicki, “Correlations Between Cyberspace Attacks and Kinetic Attacks,” in *2020 12th International Conference on Cyber Conflict (CyCon)*, Estonia: IEEE, May 2020, pp. 199–213. doi: 10.23919/CyCon49761.2020.9131731.