International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 2, February 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Internet of Things

Akilandeshwari. K, Mohanapriya. S, Sandhyia Sri. R

Sri Krishna Adithya College of Arts and Science, Tamil Nadu, India

ABSTRACT

The Internet of Things (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. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", covering devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smart phones and smart speakers.

How to cite this paper: Akilandeshwari. K | Mohanapriya. S | Sandhyia Sri. R "Internet of Things" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.715-720, URL: www.ijtsrd.com/papers/ijtsrd29939.pdf

IJTSRD29939

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

1. INTRODUCTION of IOT:

The term "Internet of things" was likely coined by Kevin Ashton of Procter & Gamble in 1999. First he prefers the name "Internet *for* things", as it requires radio-frequency identification (RFID) as essential to the Internet of things, which would allow computers to manage all individual things.

Defining the Internet of things simply refers that people interact more with internet than people", Cisco Systems estimated that the IoT was "born" between 2008 and 2009*Internet of things* has been a buzzword in today's fast-paced world.

Internet of things is a core technology in today's era. Chances are you've already heard of the term - internet of things. If not, IoT is commonly known as a network of physical electronic devices connected via internet.

1.1. IOT's Applications:

The extensive set of applications for IoT devices often divided into consumer, commercial, industrial, and infrastructure space.

1.2. Consumer applications for IOT:

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities.

1.3. IOT's Smart home:

IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems. Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off.

Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted Smart homes will become as common as smart phones. The cost of owning a house is the biggest expense in a homeowner's life. Smart Home products are promised to save time, energy and money.

1.4. IOT's Elder care:

One key application of a smart home is to provide assistance for those with disabilities and elderly individuals. These home systems use assistive technology to accommodate an owner's specific disabilities. Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to cochlear implants worn by hearing-impaired users.

They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures. Smart home technology applied in this way can provide users with more freedom and a higher quality of life. The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2019, it is estimated that the EIoT will account for 9.1 billion devices.

2.1. Commercial application of Medical and healthcare:

The Internet of Medical Things (also called the internet of health things) is an application of the IoT for medical and

health related purposes, data collection and analysis for research, and monitoring. This 'Smart Healthcare', as it is also called, led to the creation of a digitised healthcare system, connecting available medical resources and healthcare services.

IoT devices can be used to enable remote health monitoring and emergency notification systems. Hospitals also as been digitalized ,and it includes digitalized machines. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialised implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It also safeguards the life of many people's. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses.

Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. These sensors create a network of intelligent sensors that are able to collect, process, transfer, and analyze valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems.

IoT applications can turn reactive medical-based systems into proactive wellness-based systems. The resources that current medical research uses, lack critical real-world information. IoT opens ways to a sea of valuable data through analysis, real-time field data, and testing. The Internet of Things also improves the current devices in power, precision, and availability. IoT focuses on creating systems rather than just equipment.

As of 2018 IoMT was not only being applied in the clinical laboratory industry, but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients, and others involved (i.e. guardians of patients, nurses, families, etc.) to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to the patient's information. Moreover, IoT-based systems are patient-centred, which involves being flexible to the patient's medical conditions. IoMT in the insurance industry provides access to better and new types of dynamic information.

2.2. Building and home automation:

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of in home automation and building automation systems. In this context, three main areas are being covered in literature.

- The integration of the Internet with building energy management systems in order to create energy efficient and IOT-driven "smart buildings".
- The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviours.

3.1. Industrial applications:

Main article: Industrial Internet of Things Also known as IoT, industrial IoT devices acquire and analyze data from connected equipment, (OT) operational technology, locations and people. Combined with operational technology (OT) monitoring devices, IIOT helps regulate and monitor industrial systems.

One way to think of the Industrial Internet is, as connecting machines and devices in industries such as power generation, oil, gas, and healthcare. It is also made use of in situations where unplanned downtime and system failures can result in life-threatening situations.

A system embedded with the IoT tends to include devices such as fitness bands for heart monitoring or smart home appliances. These systems are functional and can very well provide ease of use but are not reliable because they do not typically create emergency situations if a downtime was to occur.

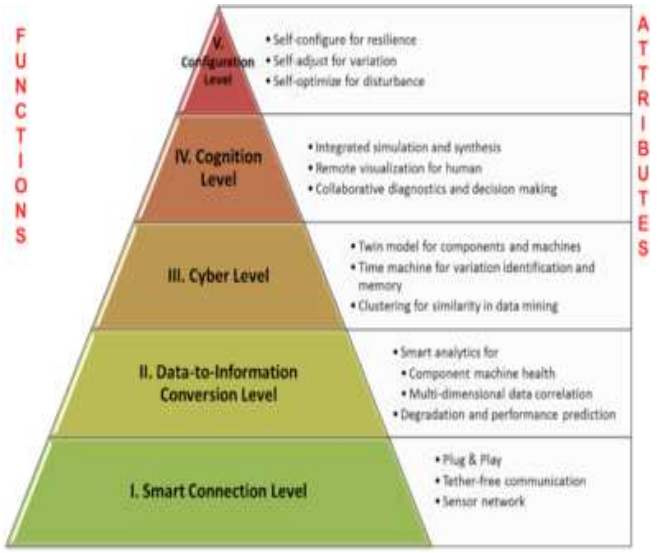
3.2. Techniques of Manufacturing:

The IoT can realize the seamless integration of various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Based on such a highly integrated smart cyber-physical space, it opens the door to create whole new business and market opportunities for manufacturing.

Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well.

The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together.

Industrial IoT in manufacturing could generate so much business value that it will eventually lead to the Fourth Industrial Revolution, also referred to as Industry4.0. The potential for growth from implementing IoT may generate $12 trillion of global GDP by 2030.



Design architecture of cyber-physical systems-enabled manufacturing system.

Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world.

Cyber-physical systems can be designed by following the *5C* (connection, conversion, cyber, cognition, configuration) architecture, and it will transform the collected data into actionable information, and also interfere with the physical assets to make process. Industrial Internet of Things (IoT) is a way to digital transformation in manufacturing. Industrial IoT employs a network of sensors to collect critical production data and uses cloud software to turn this data into valuable insights about the efficiency of the manufacturing operations.

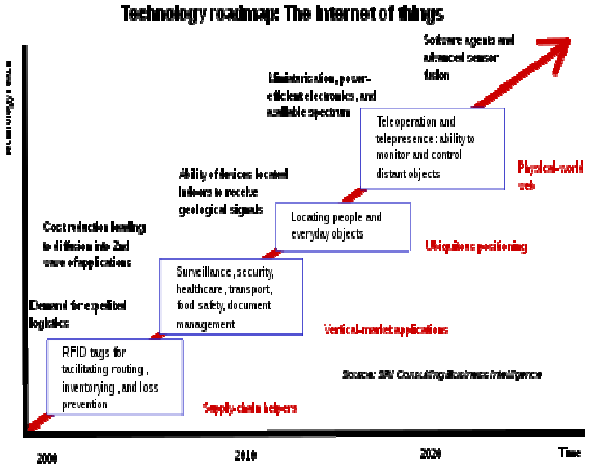
3.3. Smart farming:

Smart farming is an often overlooked in IoT applications. However, because the number of farming operations is usually remote and the large number of livestock that farmers work on, all of this can be monitored by the Internet of Things and can revolutionize the way farmers operate day to day. But, this idea is yet to reach a large-scale attention. Nevertheless, it still remains one of the IoT applications that should not be underestimated. Smart farming has the potential to become an important application field, specifically in the agricultural-product exporting countries. There are numerous IoT applications in farming such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce effort required to manage crops.

For example, farmers can now monitor soil temperature and moisture from afar, and even apply IoT-acquired data to precision fertilization programs. In August 2018, Toyota Tsusho began a partnership with Microsoft to create fish farming tools using the Microsoft Azure application suite for IoT technologies related to water management. Developed in part by researchers from Kindai University, the water pump mechanisms use artificial intelligence to count the number of fish on a conveyor belt, analyze the number of fish, and deduce the effectiveness of water flow from the data the fish provide.

3.4. Infrastructure applications:

Monitoring and controlling operations key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. The IoT can benefit the construction industry by cost saving, time reduction, of sustainable urban and rural infrastructures like bridges, railway tracks and on- and offshore wind-farms is a better quality workday, paperless workflow and increase in productivity. It can help in taking faster decisions and save money with Real-Time Data Analytics.



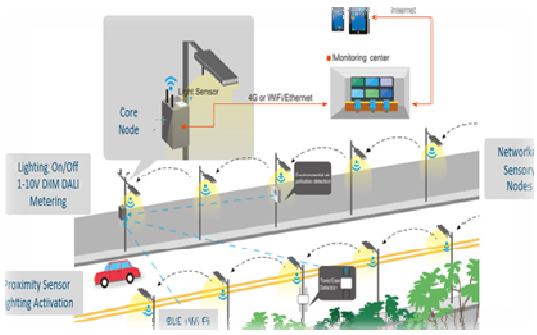
It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

4.1. Trends and characteristics:

The IoT's major significant trend in recent years is the explosive growth of devices connected and controlled by the Internet. The wide range of applications for IoT technology mean that the specifics can be very different from one device to the next but there are basic characteristics shared by most. The IoT creates opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions. The number of IoT devices increased 31% year-over-year to 8.4 billion in the year 2017 and it is estimated that there will be 30 billion devices by 2020. The global market value of IoT is projected to reach $7.1 trillion by 2020.

4.2. Management Of Smart Parking:

Smart parking management system can be used to find the vacant location for a vehicle at different public places. Smart parking's In-Ground Vehicle Detection Sensors are core technologies, playing a key part in the smart parking solution that is revolutionizing how drivers in the malls and city centers can find an available parking space. Wireless sensors are embedded into parking spaces, transmitting data on the timing and duration of the space used via local signal processors into a central parking



management application. Smart parking reduces congestion, decreases vehicle emissions, lowers enforcement costs, and reduces driver stress. For the effective deployment of smart parking technologies, each device needs to have a reliable connectivity with the cloud servers.

5.1. IOT Intelligence:

Ambient intelligence and autonomous control are not part of the original concept of the Internet of things. Ambient intelligence and autonomous control do not necessarily require Internet structures, either. However, there is a shift in research (by companies such as Intel) to integrate the concepts of the IoT and autonomous control, with initial outcomes towards this direction considering objects as the driving force for autonomous IoT. A promising approach in this context is deep reinforcement learning where most of IoT systems provide a dynamic and interactive environment.

Training an agent (i.e., IoT device) to behave smartly in such an environment cannot be addressed by conventional machine learning algorithms such as supervised learning. By reinforcement learning approach, a learning agent can sense the environment's state (e.g., sensing home temperature), perform actions (e.g., turn HVAC on or off) and learn through the maximizing accumulated rewards it receives in long term.

IoT intelligence can be offered at three levels: IoT devices, Edge/Fog nodes, and Cloud computing. The need for intelligent control and decision at each level depends on the time sensitiveness of the IoT application. For example, an autonomous vehicle's camera needs to make real-time obstacle detection to avoid an accident.

This fast decision making would not be possible through transferring data from the vehicle to cloud instances and return the predictions back to the vehicle. Instead, all the operation should be performed locally in the vehicle. Integrating advanced machine learning algorithms including deep learning into IoT devices is an active research area to make smart objects closer to reality.

Moreover, it is possible to get the most value out of IoT deployments through analyzing IoT data, extracting hidden information, and predicting control decisions. A wide variety of machine learning techniques have been used in IoT domain ranging from traditional methods such as regression, support vector machine, and random forest to advanced ones such as convolution, LSTM, and variation auto encoder.

In the future, the Internet of Things may be a non-deterministic and open network in which auto-organized or intelligent entities (web services, SOA components) and virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments.

Autonomous behaviour through the collection and reasoning of context information as well as the object's ability to detect changes in the environment (faults affecting sensors) and introduce suitable mitigation measures constitutes a major research trend, clearly needed to provide credibility to the IoT technology.

Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation, but more sophisticated forms of intelligence are requested to permit sensor units and intelligent cyber-physical systems to be deployed in real environments.

5.2. Wearables:

You would be having a fair idea of the wearable devices that are part of the IoT ecosystem and we are sure you own a few products as well. Google's famous Glass project got shelved but that hasn't shut the probabilities of what the technology has to offer. From FitBits to smart watches, anything you're wearing that is connected to the internet is part of IoT. Through sensors again, these devices communicate data to give you most precise information on your needs.

5.3. Enabling technologies:

There are many technologies that enable the IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfil.

6.1. Addressability:

The original idea of the Auto-ID Center is based on RFID-tags and distinct identification through the Electronic Product Code. This has evolved into objects having an IP address or URI.

An alternative view, from the world of the Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI.

The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers acting for their human owners. Integration with the Internet implies that devices will use an IP address as a distinct identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion different addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required.

Internet-of-things devices additionally will benefit from the stateless address auto-configuration present in IPv6, as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression.

To a large extent, the future of the Internet of things will not be possible without the support of IPv6; and consequently, the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future.

6.2 Regulation on IOT:

One of the key drivers of the IoT is data. The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage &processing of data. For this purpose, companies working on the IoT collect data from multiple sources and store it in their cloud network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems. The other issues pertain to consumer choice and ownership of data and how it is used.

A recent report from the World Bank examines the challenges and opportunities in government adoption of IoT. These include –

- Still early days for the IoT in government
- Underdeveloped policy and regulatory frameworks
- Unclear business models, despite strong value proposition
- Clear institutional and capacity gap in government AND the private sector
- Inconsistent data valuation and management
- Infrastructure a major barrier
- Government as an enabler
- Most successful pilots share common characteristics (public-private partnership, local, leadership)

6.3. Problems and controversies OF Platform fragmentation:

The IoT suffers from platform fragmentation and lack of standards situation where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications that work consistently between different inconsistent technology ecosystems hard.

For example, wireless connectivity for IoT devices can be done using Bluetooth, Zigbee, Z-Wave, LoRa, NB-IoT, Cat M1 as well as completely custom proprietary radios - each with its own advantages and disadvantages; and unique support ecosystem. Privacy, autonomy, and control. Concerns about privacy have led many to consider the possibility that big data infrastructures such as the Internet of things and data mining are inherently incompatible with privacy. Key challenges of increased digitalization in the water, transport or energy sector are related to privacy and cyber security which necessitate an adequate response from research and policymakers alike.

6.4. Data storage:

A challenge for producers of IoT applications is to clean, process and interpret the vast amount of data which is gathered by the sensors. There is a solution proposed for the analytics of the information referred to as Wireless Sensor Networks. These networks share data among sensor nodes that are sent to a distributed system for the analytics of the sensory data.

Another challenge is the storage of this bulk data. Depending on the application, there could be high data acquisition requirements, which in turn lead to high storage requirements. Currently the Internet is already responsible for 5% of the total energy generated and a "daunting challenge to power" IoT devices to collect and even store data still remains.

7.1. Security:

IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world. The hacking of baby monitors, smart fridges, thermostats, drug infusion pumps, cameras and even assault rifles are signifying a security nightmare being caused by the future of IoT. So many new nodes being added to networks and the internet will provide malicious actors with innumerable attack vectors and possibilities to carry out their evil deeds, especially since a considerable number of them suffer from security holes.

7.2. AI-Built Security Issues:

Although the threat magnitude of ransom ware has already grown 35 times over the last year with ransom worms and other types of attacks, there is more to come. Derek Manky, global security strategist at Sunnyvale, Calif.-based Fortinet agrees that the problems for cloud vendors are only emerging.

7.3 Safety:

IoT systems are typically controlled by event-driven smart apps that take as input either sensed data, user inputs, or other external triggers (from the Internet) and command one or more actuators towards providing different forms of automation. Examples of sensors include smoke detectors, motion sensors, and contact sensors. Examples of actuators include smart locks, smart power outlets, and door controls. Popular control platforms on which third-party developers can build smart apps that interact wirelessly with these sensors and actuators include Samsung's Smart Things, Apple's Home Kit, and Amazon's Alexa, among others.

A problem specific to IoT systems is that buggy apps, unforeseen bad app interactions, or device/communication failures, can cause unsafe and dangerous physical states, e.g., "unlock the entrance door when no one is at home" or "turn off the heater when the temperature is below 0 degrees Celsius and people are sleeping at night". Detecting flaws that lead to such states, requires a holistic view of installed apps, component devices, their configurations, and more importantly, how they interact.

7.4. Conclusion:

In conclusion IoT is the concept in which the virtual world of information technology connected to the real world of things. The technologies of IoT such as RFID and Sensor make our life become better and more comfortable. The IoT has the potential to dramatically increase the availability of information, and is likely to transform companies and organization in virtually every industries around the world.

Links and References:

1. R. Howells, "The Business Case for IoT", June 2015, [online] Available: http://scn.sap.com/community/business-trends/blog/2015/06/18/the-business-case- for-iot.
2. D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything", Apr. 2011, [online] Available: www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
3. L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A Survey", *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010, [online]

Available:

[1] www.sciencedirect.com/science/article/pii/S1389128610001568

[2] https://hal.inria.fr/docs/00/64/21/93/PDF/IotMiddleware.pdf

[3] https://www.thinkmind.org/download.php?articleid=icns_2015_3_40_10126

[4] http://epubs.surrey.ac.uk/716727/1/CameraReady_KAMIoT.pdf

[5] http://epubs.surrey.ac.uk/127271/1/fedcsis_woss_113_CameraReady.pdf

[6] https://www.researchgate.net/profile/Andrei_Gurtov/publication/258994707_Deployment_of_Smart_Spaces_in_Internet_of_Things_Overview_of_the_Design_Challenges/links/00b495299036f6c53b000000.pdf

International Journal of Trend in Scientific Research and Development
IJTSRD
International Journal of Trend in Scientific Research and Development
ISSN: 2456-6470