INTRO

IOT is a concept in which objects that are used in our daily life are connected with sensors, software, and network connectivity to collect and exchange data and information. These interlinked/interconnected devices enable a network of intelligence, letting us monitor, optimize, and improve various processes. IOT can be anything around us, it can be a lock, a fitness tracker, a light bulb. There are no limitations in IOT filed for being called an IOT device. To call an object an IOT device the device should be minimally using sensors and other parts hardware wise. But as in software Pov, the device should be smart enough to process some sort of data, and also be able to access the internet. Which is the main feature of an IOT device. The internet connection can be achieved by a physical LAN, WIFI, Bluetooth, or cellular connectivity. Which is the main feature of an IOT device.

In the era of technology IOT plays a vital role in making our daily life easier, efficient and time saving, energy saving and convenient. It has the power to revolutionize many sectors like healthcare, agriculture, transportation, industry, education and many more fields, IOT has been used all over the world in sectors of technology which made it a common practice.

As IOT is used in many fields, some of the basic fields that IOT is used and has revolutionized are mentioned bellowed.

1) HEALTHCARE: IOT has changed the whole health care sector, by enhancing patient care by monitoring vital signs, tracking medication intakes and timing, and by providing real-time data to the professionals which automatically results in better results and treatment plans for the patients.

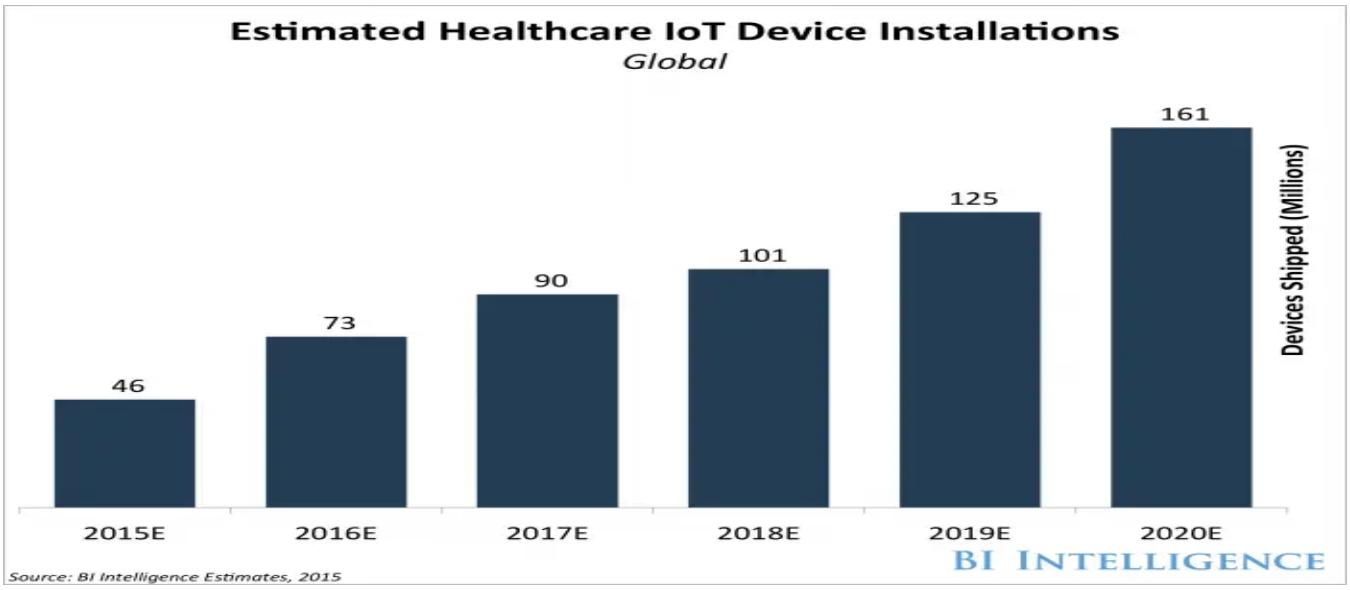


Fig:(Increasing use of IOT devices in HEALTHCARE sector)

2) AGRICULTURE: IOT device can be used to monitor soil conditions, crop health's, automatic irrigation, and pesticide usage warning. This helps the agricultural sector too much for better crop yields and more efficient and cheap practice.

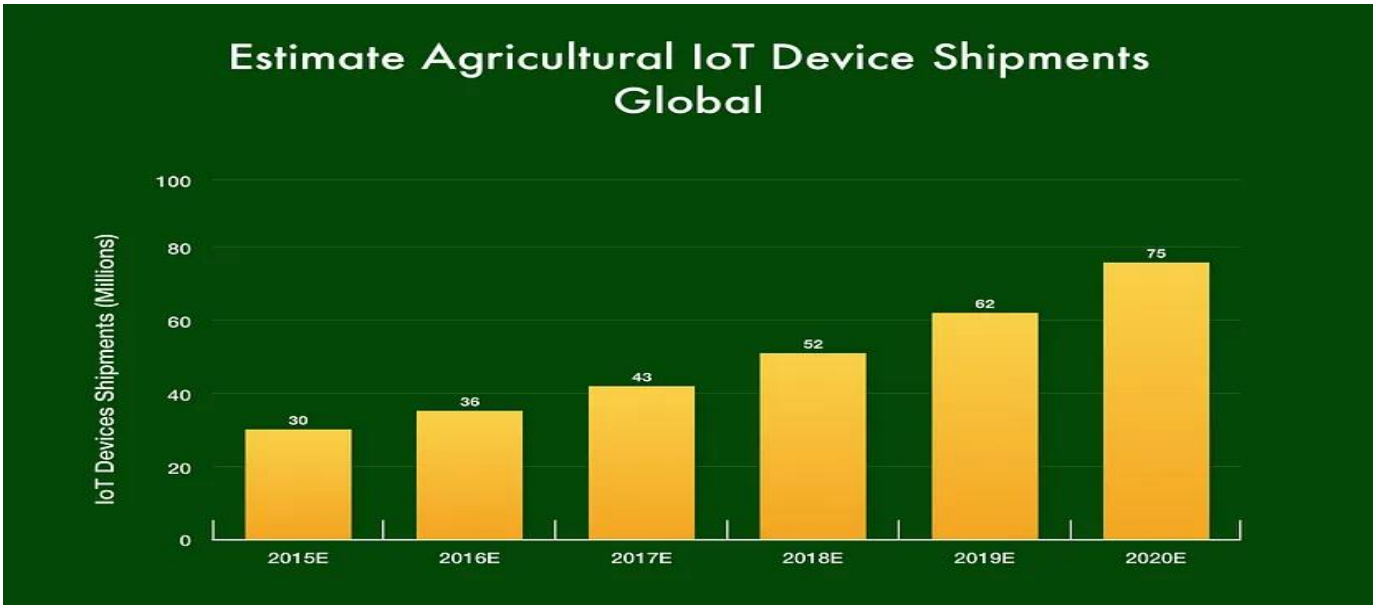
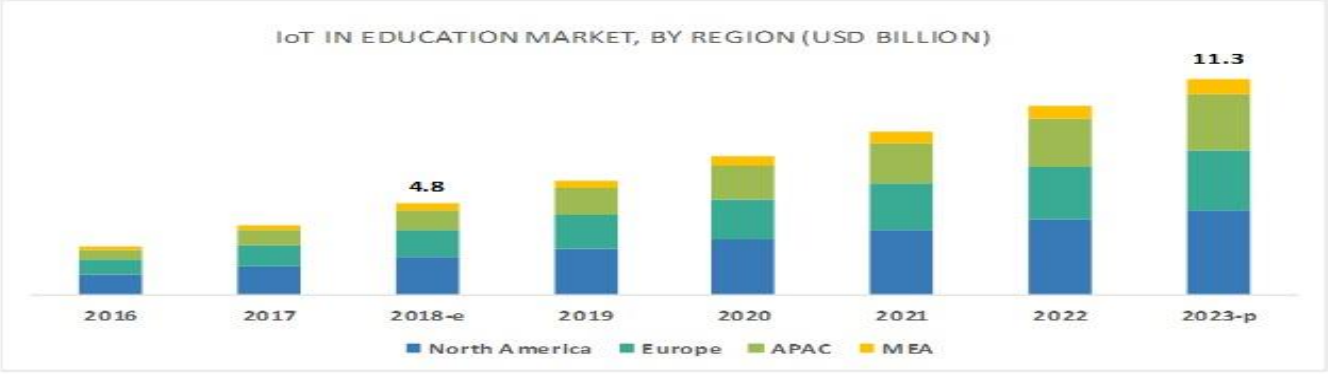


Fig:(Increasing use of IOT devices in AGRICULTURAL sector)

3) EDUCATION: IOT also can be used to enhance learning experience for students and teachers in the educational sector, as there are interactive classrooms and devices. Which results in a better education system and productive students. It can be cost efficient for both the parents and the administration, and they can provide quality education without paying heavy fees because of the cost efficiency of IOT devices.



Source: MarketsandMarkets Analysis

Fig:(Increasing use of IOT devices in EDUCATION sector)

4) INDUSTRY: IOT holds significant potential in the industrial section. It can be used to monitor and control industrial processes, optimize efficiency and productivity. It also helps to collect real time data from sensors, business can skyrocket by proper use of these devices. Management and supply of goods also can be handled by IOT devices.

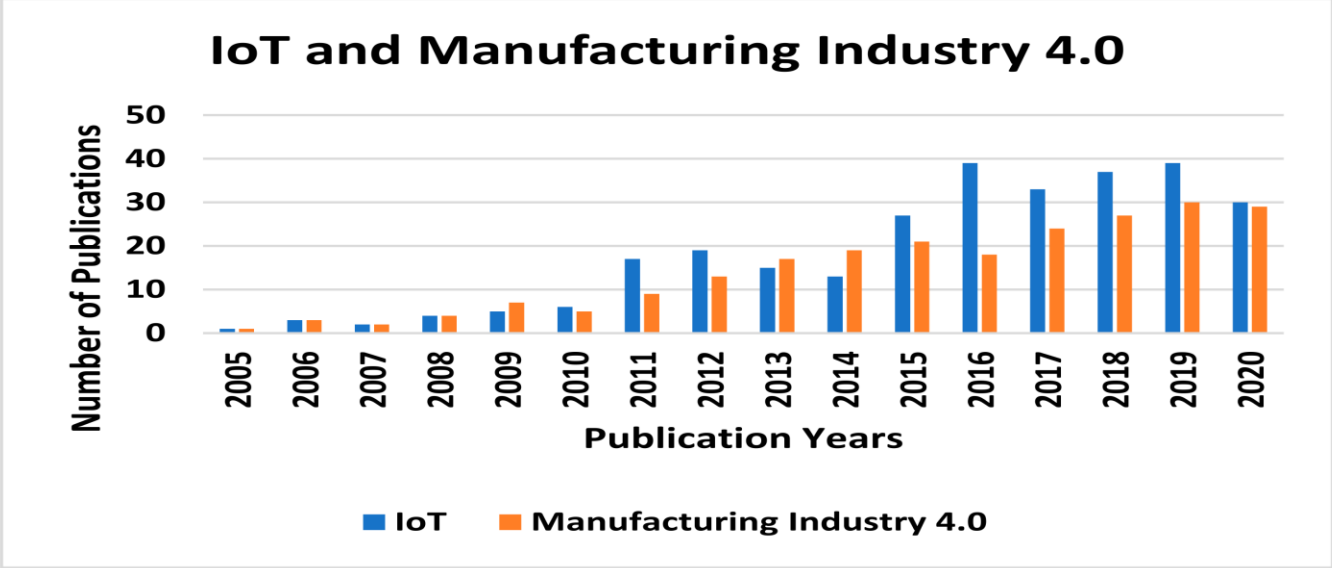


Fig:(Increasing use of IOT devices in INDUSTRY sector)

ADVANTAGE OF USING IOT:

Enhanced Security: IOT devices can be used to monitor and apply various security measures in different environments. Like keeping track of access points, identifying threats, alerting security.

Reduced Costs: By optimizing resource utilization, lowering maintenance costs, and reducing the risk of equipment breakdowns through preventative work IOT devices have brought about an era where no one needs to suffer any longer, "Crop" is no longer just crop. crop-growing efforts and efficiency has been minimized, less manpower is needed to monitor the soil, crop health. So now the production is at its best.

Increased Efficiency: IoT Technology can optimize processes in real time. All kinds of different devices are linked to the Internet. This enables enterprises to make decisions based on their own data, improving efficiency and increasing productivity.

Enhanced Analytics: IoT Technology can gather vast amounts of data from different devices and sensors. Businesses can then perform complex data analysis to strip off its outer layers of meaning. A lot deeper understanding into their information stashed under all kinds of smokey mirrors.

Customizable and Adaptable: Businesses can adjust their systems to unique needs and requirements using IoT technology, which helps in a versatile and flexible solution which is easier to update and modify as per need

Compliance and Regulatory Benefits: The application of IoT technology can improve adherence to industrial rules and regulations. Businesses can lower the risk of non-compliance and preserve correct records by offering real-time monitoring and management capabilities.

Improved User Experience: IoT devices can enhance the user experience by providing real-time data and information. For example, IoT devices can be used to control the temperature in a room or to provide real-time information about the weather.

Disadvantage of IOT:

Cost of equipment: though IOT devices may be cheap but some of the rare sensors and equipment may be expensive, which costs the user a fortune.

Data quality and Accuracy concerns: IOT devices may produce large amounts of data but cannot be assured of accuracy and quality. This is particularly for healthcare and vehicles where the accuracy of data is critically needed.

Dependence of internet: As IOT devices are supposed to connect to the internet, they are highly dependent on the internet. When the internet has low connectivity, or connectivity issue the usefulness of IOT devices might be limited.

Durability: As IOT devices are made up of sensors and other equipment, they might not be durable, some might be damaged by heat, wind or humidity. Sometimes human error can damage goods. So, they are not that durable to physical damage. so, durability is also a problem.

POSSIBLE THREATS IN IOT

Theft of data: The unauthorized access of sensitive data is a threat in itself. IOT devices generate large amounts of data making them a huge attraction for attackers. If the attacker gets access to data, they could misuse it in various ways like identity theft, fraud, extortion. Attackers can intercept the data transmitted between IOT devices, by hacking into legitimate IOT device firmware.

Malicious Applications: Hacker creates a malicious application and install them to IOT devices which automatically collects the data from device and transfers it to the attacker's server. and the attacker uses the data to blackmail or sells it for a good amount.

Unsecured IoT Devices: If an IoT device has weak or default passwords and has lack of good encryption, or is accessed in unsecured networks; attackers can easily exploit these weaknesses to gain access to the device's data

Physical Tampering: IOT devices are also vulnerable to physical tampering; Attackers can physically tamper with the device if it's not well secured or under supervision. It can be damaged or stolen.

Supply Chain Attack: cyber threats are not only risky for devices but also for the software, firmware, and even supply chain leading to installation of malicious program in device and modify it.

Distributed Denial of Service (DDoS) Attacks: In IOT; the large number of devices connected to the internet can make it easier for attackers to launch DDoS attacks. By flooding the internet with requests, attackers can disrupt services and cause network congestion.

Spyware and Malware: Spyware and malware can infiltrate the IOT devices through software vulnerabilities, and leaving the devices open to unauthorized surveillance, tracking, control, or, other illegal actions.

Remote attack: Many IoT devices offer remote access; enabling cybercriminals to remotely control, manipulate, or monitor IoT devices. This can lead to a range of potential security risks, such as device theft, ransomware attacks, or disruption of critical infrastructure services.

Insider threats: Because IoT devices are frequently deployed in environments with few or no security measures in place, the likelihood of insider threats such as sensitive information theft, industrial spying, or other malicious activities carried out by individuals with authorized access to IoT devices as well as their networks, rises.

Outdated software and firmware: When IOT devices runs outdated software, they get exposed to new vulnerabilities; which gives the attacker an opportunity to violate and tamper the IOT device.

SOLUTIONS

There are many possible threats in IOT too, because IOT is easily vulnerable for attackers to attract in this Cyber threatened world, To be safe from these types of threats possible solutions can be used, which are mentioned below:

Using secure firmware: Regularly update the firmware on IoT devices to patch known vulnerabilities and reduce the risk of attacks.

Using Firewalls and Intrusion Detection Systems (IDS): IOT devices can utilize firewalls to prohibit unauthorized access, while IDS can assist identify and prevent malicious attacks on IOT devices.

Secure data transmission: Using secure protocols like HTTPS or MQTT instead of TLS/SSL to transfer encrypted data between IoT devices and the internet; can be useful and unauthorized access to data from attackers can be prevented.

Using Strong Access Control: we can create strong and secure password for access control. The stronger the password higher the security for the IOT devices, secure authorization access plays a vital role in IOT security. This way the attackers won't be able to unauthorized access into the device.

Implanting/Implementing Threat Intelligence in IOT: We can program the IOT devices to differentiate between non-threat and threat to identify them, by feeding the IOT devices the information about the emerging threats, and upcoming vulnerability possibilities we can make them more secure and better.

There are many other ways to increase security and eliminate threats for IOT. Users and developers should acknowledge the risk of lack of security in IOT devices and their importance. There should be Awareness about the potential threats; which can be useful to minimize the risks for IOT devices.

CONCLUSION

In conclusion, the whole future of IOT depends upon the developers, manufacturers and users. It is crucially becoming a need in many sectors as of its advantages, which is really changing the whole scenario of the industry. IoT has the power to transform whole sectors of the economy, boost productivity, and improve quality of life. but as the IOT technology is developing day by day, serious security threats are arose. We can create a secure IoT ecosystem by tackling these risks with possible measures, like strict authorized access, Firewall etc. To maintain system security and encourage more innovation, it is better to keep up with time as the IOT technology is rapidly upgrading. IOT is helping to improve the quality of output produced by any industry.

Just like how IOT technology is rapidly growing, Cybersecurity landscape is also growing simultaneously and keeping update with the changes. Which makes IOT vulnerable to attacks like Distributed denial-of-service (DDOS), Ransomware, Man in the middle etc. Furthermore, comprehensive security audits, cloud-based security solutions, and frequent firmware updates can all contribute to continuous defense against new threats. To further increase the resilience of IoT devices and infrastructure against cyberattacks, it is recommended to cultivate strong relationships with manufacturers of IoT devices and establish comprehensive incident response plans. So the developers and user should focus on investing in the IOT devices. This will make IOT components and devices expensive but efficient. Security concerns are vital for its long-term success.

REFERENCE

https://www.researchgate.net/publication/320532203_Internet_of_Things_IoT_Definitions_Challenges_and_Recent_Research_Directions

https://www.scirp.org/journal/paperinformation?paperid=108574

https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT