ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

# Industrial Internet of Things

[1] Sk.RaziyaSultana, [2] R.Tejaswini, [3] Nema
[1][2][3]Department of Computer Science and Engineering
[1][2][3] G.Narayanamma Institute of Technology and Science (For Women)
Shaikpet, Hydeabad-500 104

***Abstract* - In today's world the usage of internet,computers and smart devices have become a part of our daily life. We can connect the devices to the internet and keep track of the devices .With the help of IoT we can work in a more efficient manner. The Internet of Things sits at the intersection of sensors, networks, design, business models, and a wide range of industries. At its simplest, the IoT is the idea that wireless communication and digital intelligence can be embedded into everything around us clothing, vehicles, buildings, flowerbeds, even the ground beneath our feet. Today, it is entirely possible to remotely monitor machines, perform diagnostics, acquire and calculate overall equipment effectiveness (OEE) data, upload production data and download recipes using Industrial IoT , called IIoT**

## INTRODUCTION

What is IoT?

Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. The 'thing' in IoT could be a person with a heart monitor or an automobile with built-in-sensors, i.e. objects that have been assigned an IP address and have the ability to collect and transfer data over a network without manual assistance or intervention. The embedded technology in the objects helps them to interact with internal states or the external environment, which in turn affects the decisions taken.

Why IoT?

An article by Ashton published in the RFID Journal in 1999 said, "If we had computers that knew everything there was to know about things - using data they gathered without any help from us - we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory." This is precisely what IoT platforms does for us. It enables devices/objects to observe, identify and understand a situation or the surroundings without being dependent on human help.

Different names for industrial IOT are Industrial Internet (GE) ,Internet of Everything (Cisco) ,Industry 4.0 (Siemens) ,Industrial Internet of Things (Echelon).

What is Industrial Internet of Things?

When these IoT capabilities are implemented in the Industrial and Manufacturing space, it becomes Industrial IoT. This technology is an amalgamation of different technologies like machine learning, big data, sensor data, M2M communication, and automation that have existed in the industrial backdrop for many years.

Industrial Internet makes a connected enterprise by merging the information and operational department of the industry. Thus improving visibility, boosting operational efficiency, increases productivity and reduces the complexity of process in the industry. Industrial IoT is a transformative manufacturing strategy that helps to improve quality, safety, productivity in an industry.

IIoT is about connecting industrial sensors, transducers and actuators.

Sensors: light, radiation, time, pressure, temperature, frost, humidity, rain, occupancy, CO2, gas concentration, PH, conductivity, air velocity, fire & smoke etc.

Actuators: switches, motors, dimmers, relays, circuit breakers, door locks, elevator controls, audio indicators, pumps, valves, burners, filters etc.

The IIoT is transforming industry —changing the way industries work. Whether it's enabling predictive analytics to detect corrosion inside a refinery pipe, or providing real-time production data to uncover additional capacity in a plant, or driving visibility and control over your industrial control systems environment to prevent cyber attacks, the IIoT—and the software solutions powered by it—are driving powerful business outcomes.

### IoT vs IIoT

IoT is mostly about human interaction with objects. Devices can alert users when certain events or situations occur (the temperature in the house dropped below 68 degrees), people can monitor activities and conditions from anywhere in the world, and users can control or trigger actions from a far (turn up the heat and turn on the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

driveway lights a half hour before you arrive at your cabin).IIoT also monitors activities and conditions and provides remote control functions, but these capabilities can extend far beyond what IoT currently provides IIoT technology is commonly used to monitor and control production processes while capturing detailed data for quality management and documentation. Manufacturing execution systems are embracing IIoT technology to enable closer monitoring of more parameters and more sophisticated control of processes and quality as a result.
The primary characteristic of both IoT and IIoT is the availability of inexpensive, intelligent, connected devices. IoT uses these devices for consumer convenience. IIoT uses -- often more sophisticated -- devices to extend existing manufacturing and supply chain monitoring and management systems to provide broader, more detailed visibility and enable automated controls and increasingly accomplished analytics.

***Industry 4.0 and the industrial internet of things:***

Industry 4.0 was introduced in 2011 as a German government initiative dedicated to ensured competitiveness for the manufacturing industry. The term is used to identify the fourth industrial revolution, preceded by revolutions in mechanical production, mass production, and information technology. While both IoT and IIoT operate at a business level, Industry 4.0 remains a primarily government and academic-based movement, with minimal private business involvement.

Industry 4.0 began as a high-tech strategic initiative to promote computerisation within manufacturing. Heralding the shift from centralised to decentralised manufacturing, Industry 4.0 integrates IoT, data, and services. Simply put, Industry 4.0 leverages cyber-physical systems to create networks where connected devices can talk to each other.
IIoT is the use of IoT technologies across industries. In the field of manufacturing, IIoT is fostering great leaps of innovation. For instance, Airbus, the European aircraft manufacturing giant, is using IIoT to create a cyber-physical system whereby workers can use a tablet or 'smart' glasses to scan an aircraft and determine certain specifications like what type of bolt needs to be installed. This information is then sent to robotic tools for execution. Smart factories, precision farming and proactive equipment monitoring are some other examples of IIoT at work.

Interestingly, innovation in IIoT is creating new fields such as telerobotics whereby semi-autonomous machines can be remotely controlled by humans using a virtual interface. IIoT-enabled manufacturers can use telerobots to execute tasks in dangerous environments such as inspecting underwater pipelines, conducting maintenance on power lines, decommissioning chemical plants, etc. With innovations such as these, predictions that by 2030, IIoT could generate $12 trillion towards the global GDP are not surprising.

***Early adopters reap benefits***
Industry 4.0 leverages IIoT technologies in manufacturing. By providing automation and data exchange, Industry 4.0 helps manufacturers decentralise decision-making, ensure information transparency, promote technical assistance between machines and humans, and create an environment of interoperability. A 2016 study by Forbes shows that 86 percent of companies adopting Industry 4.0 expect higher profits from lower costs and increased revenue

## MAJOR DRIVERS

Key Drivers of IIoT solutions

***1.Business outcome definition and alignment***
Defining the desired business whether it is operational efficiency by reducing costs or defects, or increasing revenue is key to designing the right IoT solution. Aggregate the data and align your project with the business objective in mind.
Key questions to ponder for designing the IIoT solution are:1.What devices, endpoints and hubs are the source of usage for my product or service?2.How are my customers and partners interacting with these touch points and what does the usage data tell me?

***2. Increase in customer and business engagement***
Enterprises have a window into customer usage patterns of their products, and they can provide better service if there was a service request during the warranty period and have the opportunity to proactively address future issues.
Analytics and Machine Learning algorithms in smart connected products can improve output, utilization and overall efficiencies of the product. Improved first-time fix rates and reduced service calls are a few key benefits of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

an analytics driven, algorithmic approach to addressing issues.

***3.Betterdesign***

Manufacturers can gain insights into product or equipment usage, which can be used for additional insights into product design of future versions. Usage data provide valuable insights and reduce over engineering costs for example. The underlying principles of solution design should support product upgrades, extensions and customizations that allow quick turnaround of a batch production to selectively enable new features in specific markets. These could be enabled by software or even small incremental hardware modules designed to provide features, gleaned from insights of product usage.

***4. Expand the Ecosystem***

IoT technology has had a major imapct in enterprises on improved equipment uptime and availability, remote diagnostics, reduced operational costs and new channels of revenue spurred by product as service models. As whole range of benefits can be realized leveraging IoT solutions,resulting in new business models and services

**BENEFITS OF INDUSTRIAL IoT**

The IIoT can greatly improve connectivity, efficiency ,scalability, time savings and cost savings for industrial organizations. Companies are already benefitting from the IIoT through cost savings due to predictive maintenance, improved safety, and other operational efficiencies. Business leaders can use IIoT data to get a full and accurate view of how their enterprise is doing, which will help them make better decisions. Some of the major benefits of IIoT are:

***1. Safety:*** This might not be the first thing that comes to mind when you think about the IIoT. Nevertheless, Companies can use all the help they can get when it comes to plant safety.

Rockwell Automation's Dave Krieger gave the talk at this year's EHS Today Safety Leadership Conference, noting, "Safety has always been there, but not one has ever really collected data. That could help in compliance and audited".

It could also help with the bottom line. For example, by tracking safety events that lead to downtime, Companies may be able to identify trends and put measures in place to prevent them from happening.

***2. Security:*** Security will be the limiting factor on how much IoT technology is deployed. With security the traditional trade-off features, but it is certainly part of the equation. An operator striving for an industrial IoT (IIoT) network must look at SCADA security, the Convergence of Operations Technology(OT) and Information Technology(IT), and make a thorough assessment of What Will allow them to achieve a secure data communications network and where they want to be in this triangle.

***3. Reliability:*** As the IoT rapidly takes hold many innovative applications are leaping ahead, bringing added complexity. Automation systems have now become as computerized and complex as any other industry system. Consequently, production cost have been reduced while operational safety levels have increased. Networked communications have centralized automated process management, further reducing costs. As a result of this networking, the subsystems controlling the individual automated processes have also become objects on Iot. The Internet and its suppliers via the Internet, and the many company's network security must be robust enough to protect company data and trade secrets. Moreover, it has to prevent unauthorized access and hacking of the Ethernet-connected SCADA network.

***4. Efficiency:*** "Smart grids can store or sell business power to the energy industry to reduce manufacturing costs. The IoT can track vehicles, monitor factory systems and enable M2M communications for more efficient manufacturing processes".

We are already seeing a huge impact on worker safety and operational efficiency in facilities that are implementing industrial IoT solutions. Despite this, 43% of manufacturers either don't understand IoT or don't know about it. IoT is something that smart manufactures cannot ignore if they want to be competitive in the rapidly changing industrial landscape.

***Challenges of the IIOT:***

Interoperability and security are probably the two biggest challenges surrounding the implementation of IIoT. As technology writer Margaret Rouse observes, "A major concern surrounding the Industrial IoT is interoperability between devices and machines that use different protocols and have different architectures." Ignition is an excellent solution for this since it is cross-platform and built on open-source, IT-standard technologies.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

Companies need to know that their data is secure. The proliferation of sensors and other smart, connected devices has resulted in a parallel explosion in security vulnerabilities. This is another factor in the rise of MQTT since it is a very secure IIoT protocol.

***Technology:*** This part is covering all technologies needed to make IoT systems function smoothly as a standalone solution or part of existing systems and that's not an easy mission, there are many technological challenges, including Security, Connectivity, Compatibility & Longevity, Standards and Intelligent Analysis & Actions.

***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 the radio in your car are signifying a security nightmare being caused by the future of IoT.

Connectivity: Connecting so many devices will be one of the biggest challenges of the future of IoT, and it will defy the very structure of current communication models and the underlying technologies. At present we rely on the centralized, server/client paradigm to authenticate, authorize and connect different nodes in a network.

***Evolution of IIoT:***

We are approaching the advent of the Industrial Internet of Things as an "evolution," rather than a "revolution.

1.Industry 1.0(1784)-The invention of steam engine kick started the indusrty1.0. At this stage people were worried about their job security as machines might replace them but in the following process it has generated new job opportunities.

2.Industry 2.0(1870)-Henry ford introduced assembly lineproduction in a car manufacturing plant to improve the production.

3.Industry 3.0(1969)- It involved the advancement of technology and led to the industrial automation.

4.Industry4.0(2010)-IIoT has brought many advantages of optimisation , smart monitoring , intelligent decision making , remote diagnosis.

***Today's reality:***

1.Software, sensors and controls running today's facilities and equipment are outdated and difficult to upgrade.

2.Companies cannot readily incorporate new features and improvements. Limited integration between internal systems (managerial apps, plant data sources) and external partners creates data silos.

3.Aging operating systems and vulnerable operational technologies pose security risks because they cannot be easily retired or replaced.

4. Limited embedded computing or intelligence control at the device, product or plant level.

***Tommorow's vision:***

1.Sensors, communications and other operational technologies are working together with information technologies, most likely meshing in the cloud.

2. Standard, fast software development techniques are used to create intelligent industrial products.

3. A common data model and sensing and control architecture that supports the flow of insights and action throughout an organization and its ecosystem of partners.

4. The IIoT infrastructure is trustworthy and resilient to inevitable compromise.

***Future of IIot***

Recent estimates tell that IIoT could add more than $10 trillion to the global economy by 2030. And that number could be even higher if companies were to take bolder actions and make greater investments in innovation and technology than they are doing today.

Over the next 12 months emerging technology will drive enhanced security rollouts

More organizations are beginning to host critical infrastructure and applications in the Cloud. To further optimize processes and shorten response times, A decentralized network architecture that brings computing power closer to where data is generated and acted upon, Fog Computing enables analysis, control and there are not enough qualified applicants to take on new digital-centric, IT roles. From a business perspective, IT/OT convergence further complicates the issue

automation closer to the "Things" in the Industrial Internet of Things.

Because Fog Computing reduces the amount of data being sent to the Cloud, cybersecurity will be enhanced by reducing the threat and attack surfaces of IIoT networks. In industries where even milliseconds are vital, certain processes will move away from the Cloud and closer to the Edge.

IoT talent recruitment challenges will incentivize private enterprises to fund secondary education programs to nurture next-gen digital-workforce

The biggest challenge affecting IoT talent recruitment is the skills gap –

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

In an effort to overcome some of these challenges, we will see enterprises (not IoT vendors) to privately fund secondary education programs to help identify and create a more skilled workforce.

With the rise of Smart City initiatives, the 802.11 ah (HaLow) wireless networking protocol will over power Bluetooth in 2017 for critical infrastructure applications such as traffic management, public safety, energy efficiency and public infrastructure design.

## CONCLUSION:

shines – high-speed data transmission rates for longer distances – Bluetooth 5 falls flat. Bluetooth 5 arguably has perks of its own: low energy needs that support a longer battery life for the devices that use Bluetooth 5. When cost is factored in, Bluetooth 5 is much cheaper to implement. Additionally, while Bluetooth 5 is already up and running, HaLow is still being rolled out, and will continue to be for the foreseeable future.
So far, businesses have made progress in applying the Industrial Internet of Things to reduce operational expenses, boost productivity or improve worker safety.
Drones, for example, are being used to monitor remote pipelines, and intelligent drilling equipment can improve productivity in Although these applications are valuable, they are reminiscent of the early days of the Internet, when the new technology was limited primarily to speeding up work processes. As with the Internet, however, there is more growth, innovation and value that can be derived with smart IIoT applications.

## REFERENCES:

1. IIoT decision making with proces energy control architectures Christopher J. Smith

2. Lean six sigma approach for global supply chain management using industry 4.0 and IIoTAthulJayaram 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)