IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HANDS ON INDUSTRIAL INTERNET OF THINGS: USING INDUSTRY 4.0 BUILD ASTRONG INDUSTRIAL INTERNET OF THINGS INFRASTRUCTURE

Dr.Sudheer S Marar, Ms Sumi.M, Sreelakshmi.V
Professor and HOD, Assistant Professor, PG Student
Department of MCA
Nehru College of Engineering and Research Centre Pambady

ABSTRACT : The industrial internet of things refers to the expansion and implementation of the internet of things (IoT) in industrial sectors and applications (IIoT). By focusing on machine-to-machine (M2M) connectivity, big data, and machine learning, the IIoT allows industries and businesses to increase their efficiency and dependability in their operations. Robotics, medical devices, and software-defined manufacturing processes all fall under the Industrial Internet of Things umbrella.

Keywords : IoT, information technology, operational technology, industry 4.0, security operations center

1. INTRODUCTION

In the manufacturing business, the phrase "industrial Internet of things" (IIoT) is widely used to refer to the IoT's industrial subset. In recent years, a wide range of industrial IoT applications have been developed and deployed. Internet of Things advancements can enhance industrial processes, supply chains, products, and services. This is because it specifically includes the function of products and services, as well as industrial processes and activities, in its scope.

2. BRIDGING THE GAP WITH IIOT

The industrial internet of things (IIoT) is definedas the expansion and implementation of the Industrial internet of things (IIoT) in industrial sectors and applications (IIoT). The IIoT encompasses more than just the traditional consumer electronics and physical device internetworking associated with the IoT. It is distinguished by the integration of information technology (IT) and operational technology (OT). Operational processes and industrial control systems (ICSs) include human machine interfaces (HMIs), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and programmable logic controllers (PLCs).

Because of the convergence of IT and OT, industry can benefit from improved system integration in terms of automation and optimization, as well as better visibility of the supply chain and logistics. Remote sensors andactuators, as well as smart sensors and actuators

As part of the fourth industrial revolution, known as Industry 4.0, the IIoT is important to how cyber-physical systems and production processes will adapt with the usage of big data and analytics. Industrial equipment and infrastructures use real- time data from sensors and other sources to aid in "decision-making," allowing them to produce insights and perform specific actions. Machines can also automate jobs that were previously impossible to complete during past industrial revolutions. The IIoT is crucial in a broader sense for use cases involving networked ecosystems or surrounds, such as how cities and factories become smart cities and smart factories.

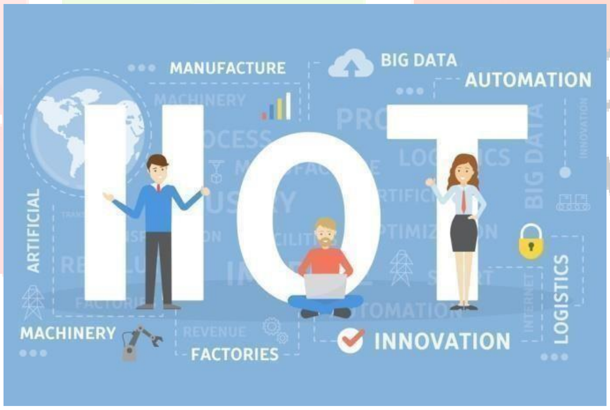

figure 1; world of industrial iot

3. ADOPTION OF IIOT: SECURITY CONSIDERATIONSAND CHALLENGES

The IIoT has the potential to reshape how industries operate, but it is difficult to have strategies in place to support digital transformation efforts while preserving security in the face of growing connectivity.

Workers' safety and product quality are important considerations for industries and businesses that deal with operational technologies. However, as OT becomes more integrated with the internet, more intelligent and automated technologies are being introduced into the workplace, posing a bevvy of new issues that will necessitate a thorough understanding of the IIoT's inner workings.

Three aspects of IIoT implementation must be prioritised: availability, scalability, and security. Because industrial operations may have been founded or in business for a long time, availability and scalability may be second nature to them. When it comes to integrating the IIoT into operations, however, many companies run into problems with security. For one thing, many companies still rely on outdated systems and procedures. Many of these have been in use for decades and have remained unchanged, making the adoption of new technologies more difficult.

Furthermore, the growth of smart gadgets has resulted in security flaws and concerns about security accountability. IIoT adopters are de facto responsible for safeguarding the configuration and use of their connected devices, but device manufacturers must secure their customers when their goods are released. Manufacturers should be able to assure user security and provide preventative measures or remedies in the event of a security breach. More importantly, as increasingly severe security incidents emerge over time, the necessity for cybersecurity becomes more apparent. When hackers get access to connected systems, they risk not only exposing the company to a huge data leak, but also shutting down operations. In order to handle both physical and digital components securely, industries and enterprises embracing the IIoT must plan and function like technology companies to some extent.

Adopters also confront the difficulty of correctly integrating industrial activities with IT, which necessitates the security of both the connection and the information. Users' data should be processed in line with existing privacy laws, such as the General Data Protection Regulations of the European Union (EU) (GDPR). While acquired data is vital for creating insights for devices and infrastructures, it is critical that personal information be separated from log data in general. Personal identifiable information (PII) should be kept in a secure database. Storing unencrypted data in the cloud with other relevant activities could put firms at risk of beingexposed.

Technology fragmentation is one of the key worries surrounding the Internet of Things, and the IIoT isn't immune to the cohabitation of diverse standards, protocols, and architectures. The uneven use of standards and protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) in IIoT systems, for example, may obstruct interoperability.

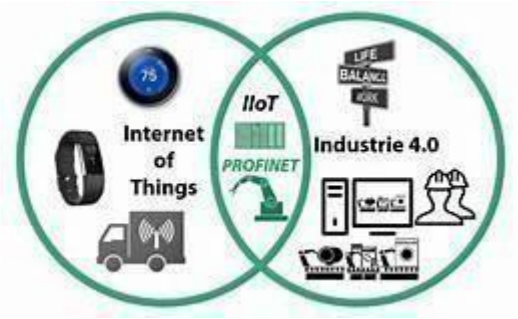

Figure2:iiot using industry4.0

4. RISKS OF IIOT INDIVERSE ENVIRONMENTS

Many of the IIoT's security issues originate from a lack of fundamental security controls in place. Exposure of ports, poor authentication processes, and outdated apps all lead to the introduction of risks. When these factors are added to the fact that the network is directly connected to the internet, new potential concerns emerge.

Businesses may have become used to the potential financial consequences of IT system failure due to cybercrime or malware infection. The integration of IT and OT, on the other hand, presents a new substantial risk factor: real-world dangers that could endanger civilians.

Unsecure IIoT systems can result in operational disruption and financial loss, among other things. There are additional security vulnerabilities in more linked environments, such as:

- Vulnerabilities in software that can be used to attack systems.
- Internet-connected gadgets and systems that are publiclysearchable.
- Malicious acts such as data breaches, targeted attacks, and hacking.
- Manipulation of systems that might interrupt operations (e.g., product recalls) or sabotage processes (e.g., production line stoppage).
- System failure that could result in device and physical facility damage, as well as injury to operators or persons nearby.
- OT systems used for extortion, as a result of the IT environment's compromise

Figure3:understanding the risk of iiot

5. SECURING OF IIOT SYSTEMS AND THE ROLE OF SOC

A security operations centre (SOC) is essential for proactively monitoring and defending against the diverse threats that affect networked environments. This centralised unit enables industries and businesses to manage the large number of warnings they may get and respond quickly.

Having a full stack of security built into the multiple layers of IIoT deployments would allow industries and businesses to perform their operations in a secure manner. The device, the network, and the cloud are all security layers.

The device layer is often made up of IIoT devices and apps from various manufacturers and service providers. Adopters of the IIoT should be able to understand how their manufacturers and service providers send and keep data. In the event of a security breach, manufacturers and service providers should be able to actively alert businesses about what has to be done.

The gateway is located in the network region and collects data from devices. Organizations should have next-generation intrusion prevention systems(IPSs) in place at this point to monitor and detect prospective assaults. A control centre that issues commands to various devices is normally located at the gateway. The control centre is the most crucial location where security hardening should be implemented to ensure protection against malware infection or hacker control.

Finally, providers should have security implementations that run server-based protection to reduce the danger of hackers exploiting servers and stored data in the cloud. This reaffirms the risk that organisations could face data protection repercussions.

As a result, securing IIoT systems necessitates linked threat defence and end-to-end security, from the gateway to the endpoint, that can:Consistent monitoring and detection of malware infections.Increased threat visibility and anomaly detection. Server and application protection in the data centre and the cloud.Threat andattack prevention between IT and OT.Data transport is encrypted.A next-generation intrusion prevention system (IPS) to keep assaults from exploiting weaknesses.

6. IOT BENEFIT AREA IN AN INDUSTRIAL CONTEXT

Two distinct IoT benefit areas in an industrial context are discussed in this section.

Non-Production Data Collection for Improving Industrial Operations:

Industrial operations are quite good at detecting production data to maintain optimal performance, but they are generally bad at integrating data from maintenance, quality control, and raw material sources into production planning, scheduling, and control concerns. The challenge of integrating such data into the manufacturing information and control system is one of the reasons. IoT has the ability to assist solve this problem by making this data available — even if it comes from third-party data providers. Conversely, some of the growing Industrial IoT products can enable the use of production data for non-production needs (maintenance, quality control, etc.).

Figure 4 depicts various manufacturing data "layers": core production data, peripheral production data,factory-wide data, supply chain data, and ecosystem data. Because of the various information systems deployed, there is currently very little interaction between these levels.

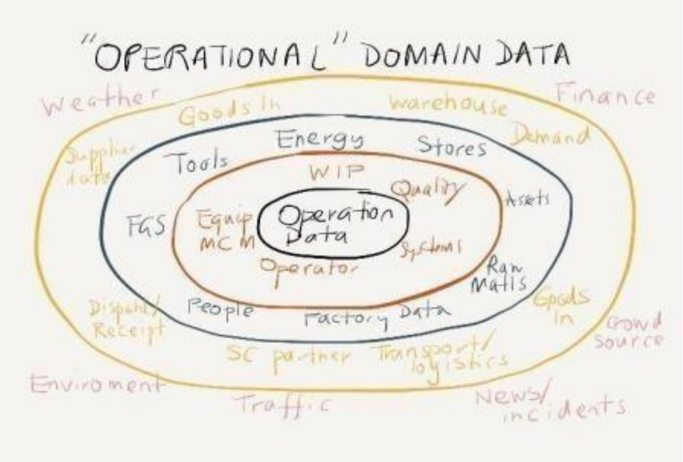

Figure 4: Layers of manufacturing relatedsensed data

Product Data Collection to Improve ProductLife Cycle Performance:

As a product travels through its life cycle, a second serious restriction of today's sensed data provision is product data and product-related process data. Databases of suppliers producers, distributors, retailers, and service providers, among others, provide fragmented information about an industrial product. Over the last 15 years, the Auto ID Centre, EPC Global, GS1 and others have worked to develop standards for the interchange ofproduct data among numerous organisations. Many of today's product lifecycle management difficulties may be addressed by an industrial IoT framework in which product data could be easily gathered and linked to a physical entity as it moved through its life cycle. It may also allow for self-managinggoods, as seen in Figure 5.

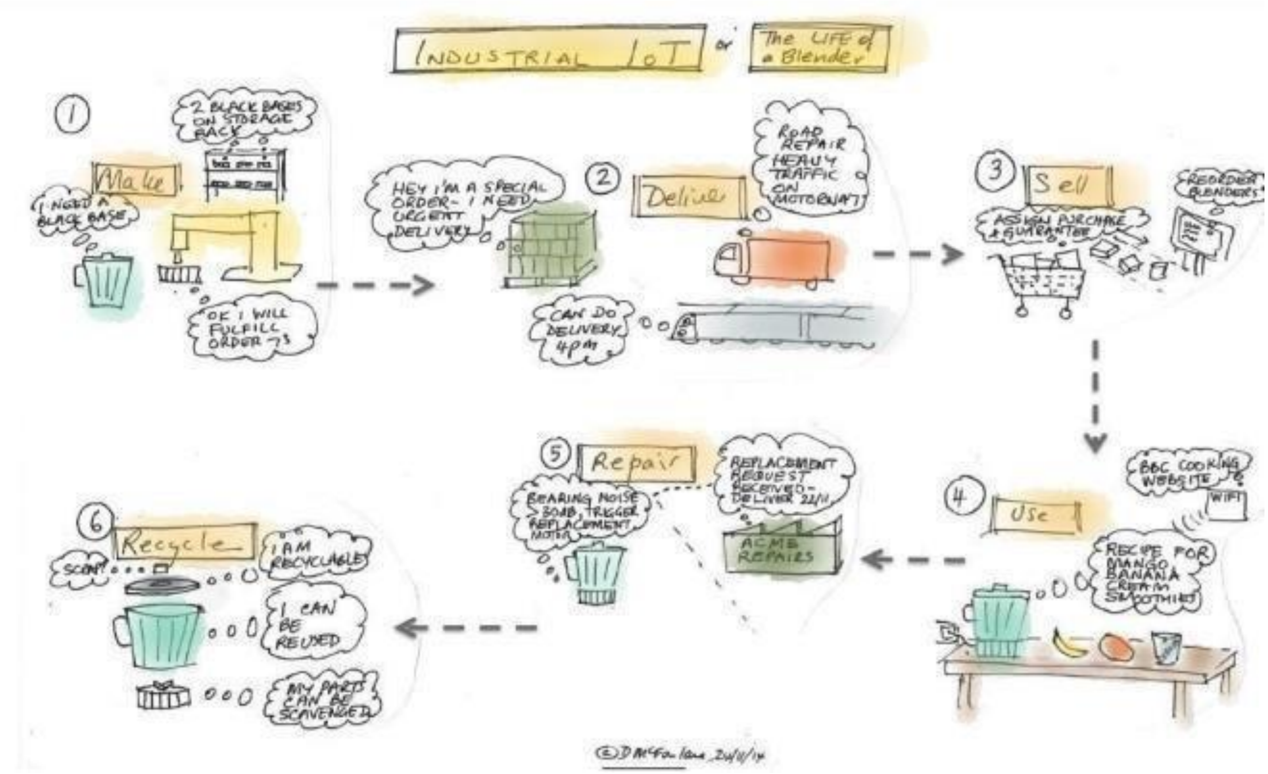
INDUSTRIAL IoT
or
The LIFE of a Blender
1
Make
I NEED A BLACK BASE
2 BLACK BASES ON STORAGE RACK
OK I WILL FULFILL ORDER 73
HEY I'M A SPECIAL ORDER - I NEED URGENT DELIVERY
2
Deliver
ROAD REPAIR HEAVY TRAFFIC ON MOTORWAY
CAN DO DELIVERY 4pm
3
Sell
ASSIGN PURCHASE & GUARANTEE
REORDER BLENDERS
4
Use
BBC COOKING WEBSITE
WIFI
RECIPE FOR MANGO BANANA CREAM SMOOTHIES
5
Repair
BEARING NOISE 30dB, TRIGGER REPLACEMENT MOTOR
REPLACEMENT REQUEST RECEIVED - DELIVER 22/11
ACME REPAIRS
6
Recycle
SCAN!
I AM RECYCLABLE
I CAN BE REUSED
MY PARTS CAN BE SCAVENGED
©D McFarlane 24/11/14

Figure 5: Industrial IoT supporting product life cycles

To summarise, applications in the following sector smay have the greatest immediate impactfrom Industrial IoT:

Bringingtogether information from suppliers,logisticsproviders, and customers

Data from new technology, peripherals, tools,andequipment are introduced.

A distributed production environment necessita- testheaddition of new data sources, locations, andowners.

Raw materials, parts, goods, and orders going through organisations are all equip-

ed with sensors

may have the greatest immediate impact fromindustrial IoT

- Bringing together information from suppliers,logistics providers, and customers
- Data from new technology, peripherals, tools, and equipment are introduced.
- A distributed production environment necessitatesthe addition of new data sources, locations,

and owners.

- Raw materials, parts, goods, and orders going through organisations are all equipped with sensors.

7. THE FUTURE OF INDUSTRIAL INTERNET OF THINGS

A short glance at the internet of things' future inindustry

A quick look at some studies from Bain & Company, IDC, and Accenture, among other reputable agencies and publications, reveals the global bullishness on the internet of things for Manufacturing($189billion)withan emphasis on asset management, transportation and worldwide freight($85 billion) with an emphasis on supply chain management and tracking, and utilities ($73 billion) with an emphasis on smart pumping andsmart grids, according to IDC Research.

By 2022, Accenture estimates that the worldwide IIoT market would be worth almost $14.2 trillion. Given growing defence spending by NATO and allied states on smart technology such as drones, armour, and first reaction and detection systems aimed at reducing human casualties in combat zones, this is a realistic figure. To summarise, the Industrial Internet of Things is a boon to the modern industrial-business complex because it allows for innovation, faster decisionmaking, informed choices, and the The Internet of Things is closer tobecoming a reality than most people believe. The majority of the essential technology advancements have already been completed, and several businesses and agencies have begun to deploy a small-scale version of it. The influence it will have on the legal, ethical, industry. Despite the recent global slowdown, Bain & Company predicts that IIoT technology would produce$300 billion in sales in calendar year 2020, compared6to$150 billion for its consumercentric IoT sibling

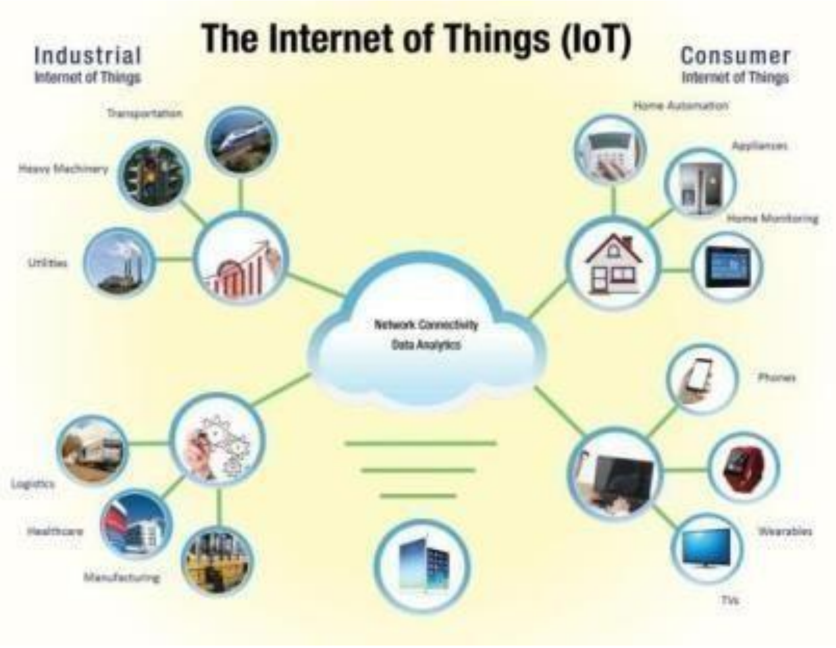

Figure6:Future of iiot

8. CONCLUSION

security, and social spheres is one of the key reasons it has not been fully implemented. Workers may abuse it, hackers may gain access to it, firms may refuse to give their information, and individuals may object to the full

.lack of privacy. As a result of these factors, the Internet of Things may be delayed longer than necessary. prediction of redundancies, all of which help modern industry become the most productive, efficient, and profitable it has ever been

REFERENCE:

[1] IIoT A Industrial Internet of Things (IIoT): Intelligent Analytics for Predictive
Maintenance ,R.ANANDAN,SUSEENDRAN Complete Guide - 2021 Edition
GERADRUSBLOKDYK (21 November 2020)

[2] IoT/IIoT Security – Risk Evaluation in Diverse Environments - InBrief
AnalysisWorldwide,BOGDAN COTOVELEA,WOLFGANG SCHWAB(19 APRIL 2021)

[3] Introduction to Industrial Internet of Things and Industry 4.0
BySudip Misra, Chandana Roy, Anandarup Mukherjee(3 FEBRUARY 2021)

[4]Industry 4.0: The Industrial Internet of Things Paperback – 4 January 2017
by Alasdair Gilchrist

[5] IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet
of Things,DAVID HANES

[6] The Internet of Things, revised and updated edition (The MIT Press Essential
Knowledge series,SAMUEL GREENGARD,(24 AUGUEST 2021)

[7] The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things,
ADITYA GUPTHA