IoTSense

# DEMYSTIFYING INDUSTRIAL IOT

-White Paper

# Demystifying Industrial IoT

*IoT or the Internet of Things is a network – Vehicles, physical devices, buildings and every other item embedded with sensors, software's, electronics for network connectivity enabling collection and exchange of data*


## About the Authors

**Sanket Khandare**, having a rich 10 years of experience in IT. A techy at heart, his key areas are IoT, Cloud, Big Data, ERP and Gamification

**Priyanka Pareek**, specializing in enterprise business analysis, complex project conceptualization, building processes and closely monitoring tech trends


## About Winjit

Winjit is a global technology solution provider. From conceptualizing, optimizing and developing conventional enterprise software systems to developing Morden day mobile apps for all consumers. Equipped with the best functional and technological resources supported by a team if expert & qualified software professionals Winjit provides its customers with cutting edge business solutions.

## Contents

# 1 Introduction to IoT

*We live in a world where there is so much to do but so little time. The multitasking capabilities of the present generation is at the highest ever rate. The market is flooded with Technology and Innovations. Yet something seems amiss, that something is "Control". Control over every Hardware, Electronics, Machine or Technology you own personally as well as professionally. The ability to start stop, monitor, and control and analyse system is what makes the world truly connected.*

Expanding control over things have been a major intent for humans ever since the advent of fire. The human breed have been ideating to invent and disrupt different sectors to makes life easier and smoother.

Connecting was another important aspect. From discovering new lands across the seas to connecting the people through the internet, the world has come a long way. But do we stop here? Off course not We see the world as a hyper connected cluster of not only humans, but humans to objects and objects to objects themselves.
This is achieved by IoT. A world which is more connected, a world which is smarter. The possibilities are endless, on what we can do and what we can achieve.

In 2008, 'things' connected to the internet were already more in number than people and by 2020 these internet connected things will have already reached 50 billion, Cisco systems further foresee profits and cost savings from IoT at $19 Trillion within the upcoming years.

## What is IoT?

An infrastructure worldwide for the information society which sanctions interconnecting at an advance level for both physical and virtual things, as defined by ITU based on existing and ever evolving practical info and communication technologies.

However this broad perspective of IoT cannot be consumed in a single universal definition.

The Core components of IoT are:

**1. Things** – Smart things (objects) with Unique address or identification

options to connectivity and networked sensors.

**2. Communication medium** – Wired & wireless (Wi-Fi, 4G, Bluetooth, ZigBee)

**3. Analytical Infrastructure** – Data Stores, Analytic Engines.

**4. Controller Tools** – Hardware or software providing complete control over the Object.

**5. Presenters** - Light / Sound indicators, alarms, or even Dashboards and reports.

Over the course of this document we discuss every aspect of IoT that you shall consider for your business.

# IoT for Industrial Use

The true potential of IoT is unveiled when it is used in the manufacturing and industrial section. Industrial Internet of Things (IIoT) combines the most powerful technologies that have been used in the industrial sector for ages. The collaboration of Machine Learning, Big Data, Sensors, Machine to Machine (M2M) communication, automation, Artificial Intelligence and IoT gives us a promising Formula for near perfect Industrial Operations. The Gigantic Industrial Machines will not just be powerful but also be smart.

The massive data set from machines when captured consistently and accurately can help businesses to identify problems and inefficiencies sooner, helping them save time, money and some critical blunders. It could leverage quality control, sustainability, optimal utilization, green practices, supply chain traceability and efficiency.

## Opportunities and benefits

Speaking of IIot, it brings about opportunities and benefits to those who are willing to adapt to the tech.High volumes of data generated through the many connected devices/products may cause severance with the increasing ability to make robotic decisions and put them into action in real time. The following research by EconomicForum [3]acknowledges that primary business contingency will be found in four major areas:

- Improved **operational efficiency (**e.g., improved uptime, assetutilization) through predictive maintenance and remote management.

- The emergence of an **outcome economy** fuelled by software-drivenservices, innovations in hardware and increase in visibility of products,processes, customers and partners

- New **connected ecosystems,** coalescing around software platforms thatblur conventional industry boundaries

- **Collaboration between humans and machines,** which will result inunparalleled levels of productivity and engaging work experiences in high numbers.

*The collaboration of Machine Learning, Big Data, Sensors, Machine to Machine (M2M) communication, automation, Artificial Intelligence and IoT gives us a promising formula for near perfect Industrial Operations.*

# IoT Adoption Stages in Industry

*While Various Organizations have accepted IoT with open arms the level of adoption in different Industries and Businesses is different. Some of them started at a very basic level and then gradually moved to Anytime Anywhere level (cloud level), while some took a bigger leap and had a kick start with thecloud level.*

The following section provides a brief overview of the different levels one can adopt

## Basic Level

A minimal level of automation is used at this level and the focus is on data capture only. This data is not utilized further to trigger any automated action. The capture data can be refined for analysis and observation by the organization depending on their needs,

## Automation Level

The information received in the above level has been sift out for interpretation.Based on the results, business processes are executed.

## Business Innovation Level

Organizationsare able to take their business to the next level using IoT innovation by integrating IoT in their products or offerings. This often requires cooperation and planning among different people and organizations that have an interest in the data and the intelligence coming from it, for example, product manufacturers, retailers and their suppliers. In this way, everyone in the data chain gets what they need in a manner most likely to yield tangible improvements to business. Anotherexample is energy providers that could have a smart grid setup allowing providers to provide electricity using different sources of energy which they could control using the IoT.

## Anytime Anywhere Level

Organi¬zations make cloud computing an enabler of the IoT. Here, data and services reside in a massively scalable cloud and can be accessed easily from any connected device over the Internet. Physical location and underlying infrastructure details are transpar¬ent to users. Anytime, anywhere access to IT resources is delivered

*IOT Adoption stages from 'Nowhere' to 'Anytime Anywhere'*

*It's important to know 'where are we' and 'where we would like to be'*

*The domains adopting IIoT are:*

- *Whole Sale*
- *Process Manufacturing*
- *Discrete Manufacturing*
- *Utilities*
- *Logistics and Retail*

# Current Problems

*A recent research shows that a whopping 94% of all businesses have seen a return on their IoT investments. [4]IIoT is destined for growth across versatile domains, however it raises significant challenges that could limit the utilization of its true potential benefits. Some of the most pressing challenges and concerns emerge from the five Key IoT issue areas, these include:*

- *Connectivity Challenge*
- *Performance and Scaling*
- *Security Issues*
- *Privacy Issues*
- *Interoperability/ Standards*

## Connectivity Challenge

Connecting things, systems, sensors, wearables and devices have brought us closer to a connected world. As we move towards a more connected world, the biggest challenge that remains is that of connectivity. Along with the value it adds, connectivity also brings in complexity.

For many engineers, the greatest challenge in designing for the Internet of Things (IoT) is connectivity. Implementing robust and secure access to the Internet or Wide Area Network (WAN) is outside their range of experience. To make design even more difficult, developers need to support access to multiple devices that are limited in their processing capability. Connectivity must also be added in a way that does not adversely impact overall system cost or power efficiency. [5]

There are design concerns when connecting complex IoT devices in a network or with a system. Different types of devices support varied interfaces and protocols. The design should not turn complex or expensive, in an attempt to overcome these challenges.

To collect and aggregate data from a disparate set of nodes requires a means for bridging devices with a range of processing capabilities andinterfaces together in a consistent and reliable way.An effective way for untangling and processing of the networking of 'things' – Gateways! Gateways perform this as they support the several ways nodes natively connect, whether this is a ranging voltage from a raw sensor, a stream of data over I2C from an encoder, or periodic updates from a machine via Bluetooth.

Gateways are a productive way to analyse the diversity of devices by combining information from contrastingsources and interfaces in turn bridging them to the Internet. Hence, the individual nodes will not have to carry the ramifications or cost of a high- speed Internet interface in order to be connected. [5]

## Performance and Scaling

Scalability is Paramount. Your IoT ecosystem should be capable of expanding as your business grows. This needs to be done, without disturbing the existing system and preventing system downtime. Instead of reinventing the entire system, the initial designs should be such that it leaves room for seamless scalability.

Performance is another aspect that gets affected by the growth of business. Your IoT system, should be powerful enough to weigh weigh the load of excessive data and if it's not, there should be provision to

# Current Problems

configure and improve the performance capability of the system as you go along.The performance at various level is monitored:

- **Physical Level: Devices, Sensors, Actuators**
- **Session Protocols Level: MQTT, CoAP, HTTP**
- **System Level: Database, processing, analytics**
- **End User Level: Business IoT, Consumer IoT**

Performance Enhancement and scalability at any of these desired level should be obtainable by the IoT ecosystem. However, predicting the scale and performance of such systems can go wrong and may bring aboutlimitations. If an IOT Sense is a part of the ecosystem, scaling and performance enhancement will be a simplified task.

## Security

The technology that IoT connects is permeant in businesses. One poorly secured IoT device can expose crucial data to theft and act as an entry point for cyber-attacks. A counter scenario is the device holding threat to the internet and other systems creating an overall unsecure environment.

As users of the Internet, we need to have a high degree of trust that the Internet, its applications, and the devices linked to it are secure enough, to do the kinds of activities we want to do online in relation to the risk tolerance associated with those activities. The Internet of Things is no different in this respect, and security in IoT is fundamentally linked to the ability of users to trust their environment. [6]

An IoT Device manufacturer is faced with many challenges right from the design of the device. Incorporating security standards and compliance at this stage is an aspect ignored due to competitive costs and technical constraints.

As the number of IoT devices keep on increasing, the possibilities of vulnerability increases too. In thehyper connected world where everything, right from your heart rate to the traffic signal to the industrial boilers are connected to the internet, security should be of utmost importance and should be considered a critical issue.

This calls for the need of effective and appropriate solutions to IoT security challenges.Some security challenges specific to IIoT are:

### Hyper connectivity

IoT devices are developed and deployed at an ever growing rate today. The existing tools methods and strategies of IoT Security should be closely refined.

### Homogeneity

The key designs, protocol or manufacturing characteristics of similar IoT devices, can generate a relay effect on the failure of a single security aspect.

### Longevity

Technology changes drastically every 5 years, it's thus required that we keep evolving and upgrading the products too. Unlike traditional systems, which have frequent OS updates, IoT is still fragile in terms of updates and enhancement post deployment. Ensuring long-term support and managing IoT devices is an important factor.

### Transparency

The complex working of IoT is something that not many users understand. Most of them are oblivion to the functions their IoT device is performing or pertaining to perform. A small function unknowingly updated

# Current Problems

by the manufacturer can lead to some intensive business damages. More visibility to the user can avert such blunders.

## Privacy Issues

As mentioned earlier, it is estimated that 50 billion devices will be connected by 2020. [1] This proliferation poses new privacy and security risks that must be assessed.As the connection between things increase the organizations are exposed to significant risks of malicious attacks, data theft, thingbots and data breach.

The exposed records can leak critical information, incurring huge losses to the businesses. Apart from this, the data is also available with the IoT service / device owner. The user of the services can be oblivious to the type and details of the data that is being sent to these third parties. This violates the basic Privacy rights and expectations of an individual or businesses.

It's critical to address the privacy problems as there is a high degree of trust factor at stake. A way to deal with this can by introducing privacy-by-design. This will give rise to privacy-respecting products and practices. There should be more transparency to the user in terms of what data is being collected by the IoT devices and how much information is shared with a third party.

There has to be fairness in data collectionand usage, an agreement between the vendors, third parties and business owner can be reached to ensure fair usage. Also there has to be a level of customization, as the privacy expectations, norms and laws for different businesses, individual and countries are different. These challenges go beyond the current data privacy issues as it is ever evolving.

A Gateway comes to rescue by offering control, and clarity. A business owner can rightfully control the flow of information and data that's confidential to the company. Strategies can be developed and integrated to meet a broad spectrum of expectations and requirements.

## Interoperability / Standards

Interoperability facilitates the ability to choose devices with the best features at the best price and integrate them to make them work together. Purchasers may be


Connectivity Challenges


Security


Performance & Scaling


Hyperconnectivity


Longetevity


Transparency


Privacy


Standards


Proprietary Ecosystem


Cost Constrains


Legacy Systems


Configuration

# Current Problems

hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, and concern over vendor lock-in, or fear of obsolescence due to changing standards. [6] Lack of interoperability results in some concerns around the IoT enabled devices:

- **Not efficiently being able to test API's using common approaches and mechanisms.**
- **Unsuccessful to push and pull information from devices using the same interfaces.**
- **Unable to secure devices using third-party security software**
- **The inability to monitor and manage devices using a common management and monitoring layer.**

According to a report "Interoperability is required to unlock more than $4 trillion per year in potential economic impact for IoT use in 2025, out of a total impact of $11.1 trillion across the nine settings that McKinsey analysed."[7]

Interoperability leads to freedom of innovation.The importance of interoperability and standards have increased with thedevelopment of the Internet of Things (IoT).

Organizations developing Standards have done a great deal of work to standardize protocols in order to simplify implementation and lower the cost of IoT products.
As a result, new protocols were developed and existing protocols were redefined in new ways with lightweight profiles. At this stage defining standards and protocols will be an evolving process and While in doing so, a number of factors are considered:

## Proprietary Ecosystems

Some manufacturer can choose to create a closed ecosystem there by eliminating the compatibility with other components from opponent vendors. On the other hand, some manufacturers see this as an opportunity of collaboration and provided protocols that help quick and easy adoption.

## Technical and Cost Constraints

These factors are considered while implementing standards. It won't be logical and economical for the manufacturer to design interoperability features into a product and test it. However, for long term products, talking about IIoT, compliance with standards leads to lifecycle gains.

## Legacy Systems

When legacy systems are Connected with new IoT devices, achieving inter-operatabilty is a big challenge as in order to maintain compatibility with legacy systems, IoT engineers are faced with design trade-offs.

## Configuration

When managing a large number of IoT devices the configuration process tends to get lengthy and complex. To simplify and ease the process the systems should be built with a thoughtful design, standardized configuration tools, methods and interface.Ensuring that the above factors are taken into consideration by each and every IoT engineer is a tricky task. However, introducing a component like a Gateway, which complies with all the interoperability standards is the way forward.In a fully interoperable environment any IoT device would be able to connect to any other device or system andexchange information as desired. [6]

# Winjit IoT Sense

There's a plethora of IoT devices available, thousands of Industrial IoT solution to choose from and hundreds ofrisks and challenges to deal with. Managing these whilst getting the desired result requires acute attention from the businesses.

Adapting a networking methodology which is robust, secure and scalable is of prime importance here and that's where IoT gateways play an important role. Gateway's task is to primarily bridge the IoT devices and the internet beyond. Connecting the IoT products which communicate via specific protocols, store and parse the information and then send them over to cloud servers for processing and analytics. [8]

## Introduction

Winjit's IoT Sense simplifies theimplementation and management of smart and secure IoT Solutions connected through the cloud. The Winjit's IoT Sense provides a flexible and innovative business transformation at an economical cost across multiple operating systems and protocols.

Geared with Intelligent analytics, this gateway coherently manages the lifecycle of an IoT deployment. Connecting to a legacy system permits IoT infrastructure, networks, embedded systems and third party apps, thus transforming businesses.

Winjit IoT Sense provides visualisation, monitoring and control through tools that are easy to handle and can be easily integrated into the exiting systems. It smoothens the interaction between smart application and services. It incorporates security and privacy on every level with an unexposed OS.

The key features are:

- A lightweight OS based on Arch Linux
- Open source API's Access
- Interactive Dashboard
- Local Analytics
- Live Data Stream to Cloud
- Scheduled Data Stream to Cloud
- Actionable Triggers & Notifications
- Offline Data Storage
- Optimised Data Sync

The Sensors to Gateway are aided throughWi-Fi, ZigBee, BLE, LoRa, Gateway to Cloud, HTTP/S. There is extensive Protocol Support for REST, MQTT, and SOAP etc.

The Winjit's IOT Sense comes with a control panel which facilities a Dashboard, Sync Management, Device & Data Management, Local Analytics, Settings and User Management.

## Device Management

The Device Management module allows to add/update/ remove devices.The Device information will have sensor type, device group, communication protocol, description, and synchronization details.The available devices listcan be sorted by type, group and status. The devices can be Enabled/disabledaccording to the usage.

## Sync management

Complete sync management can be done from the control panel and businesses can choose the synchronization service provider. A level of customization can be applied to each device from the Device Management when creating or updating device configuration.

## Dashboard/Local Analytics

An interactive dashboard that displays real-time summary and statistics such as:

- Total number of rows Sync'd with cloud
- Total number of rows received from all the devices
- Number of devices
- The Current date and time
- Data Stream Statistics: An area graph with the number of rows uploaded over time period
- A circular chart with the average monthly uploads

# Winjit's IoT Sense

Apart from these, business specific custom graphs can be generated for the connected devices. These graphs can be generated based on data streams received from the various devices.

## Data Streams

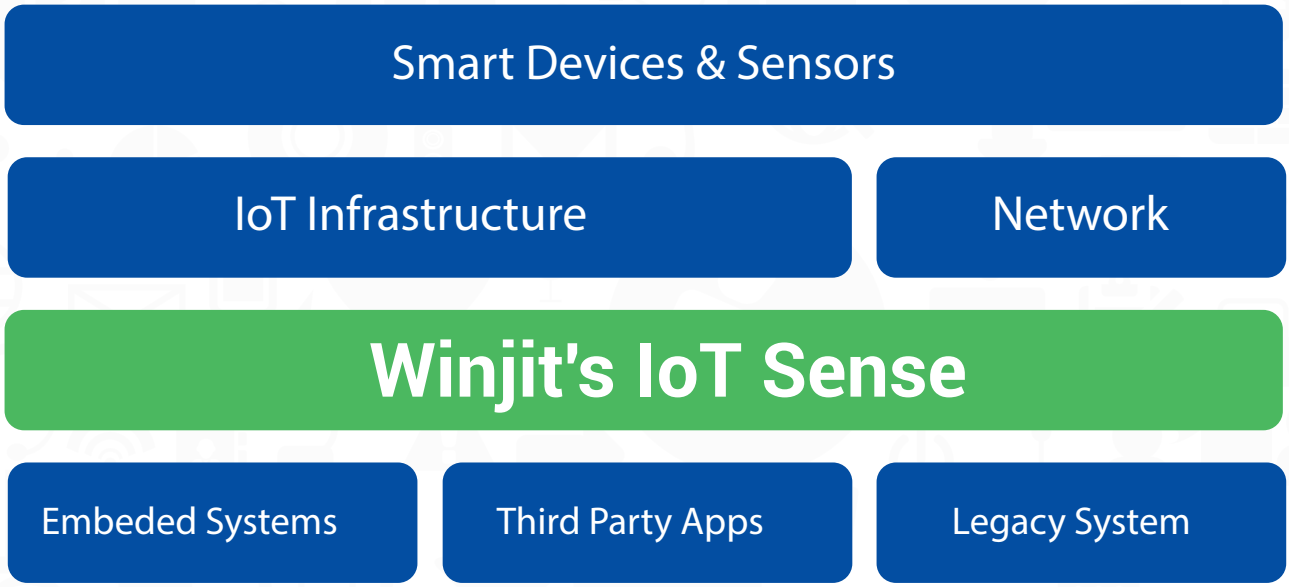
Streams of data is generated from the IoT devices and with Winjit IoT Sense the data is securely posted on the gateway. The Data streams from all your IoT devices can be accessed and searched with device ID, device Name or timestamp. The device data within specified dates can be exported.

## Triggers

Different Verticals have different needs. In order to blend theseTriggers can be added to check for a specific condition on a received data stream. A Specified action can be executed if condition is matched. The Trigger action includes REST call, Email, MQTT publish. Triggers can be enabled/disabled from the control panel.

## Open APIs

Our APIs are accessible to our partner developers fostering continuous innovation and integration. The Open APIs are well documented and available via open source contribution request to employ open technologies.



# Rapid Solution Development

Traditional deployment of IoT systems can be a slow and costly affair. But with gateways that are robust and pre-configured the, you can get your business up and running in weeks instead of months. The delivery approach is simplified using the best practices to deploy quickly, predictably and affordably.

The approach can be broken down to a series of steps to start your IOT Solution.

### STEP 1: Connect and Scale as you need

Greater risk is involved when the IoT ecosystem for your business is designed and implemented. A group of powerful devices are suddenly introduced in your existing model, leaving the system exposed and vulnerable.

Also, as your business grows, you'll need to increase the number of sensors, IoT devices, machinery and make sure that all these new components blend with the older system.

For both the above scenarios, IoT Sense ensures smooth deployment of your solution. IoT Sense offers scalability, as it grows along with your business. It enables you to add/remove N number of devices.

### STEP 2: Aggregate data on Cloud

In the ever moving pace today, it's important that we have access to data as and when we need. More importantly, the entire data should be at the same location. Storing data over cloud eliminates ambiguity, redundancy and ensures integrity.

### STEP 3: Analyse and Visualize important things

The data received needs to be processed, analysed and represented visually. The data received is cluttered information that needs to be refined in order to generate meaningful output. With the IoT Sense, Parameters can be defined based on your requirements. These parameters then define the processing type and level of the data. Once the desired data is obtained, it is then represented in the suitable visual form.

### STEP 4: Integrate within your business processes

The refined data obtained is crucial when making strategic decisions. Integrating the data points with business makes the ever so static data reap dynamic outputs. It helps stakeholders make informed cost-benefit analysis decisions

# 1 Conclusion

*In conclusion, most of the necessary technological advances needed for a hyper connected ecosystem have already been made. There are computers, sensors, and networks to monitor and control devices. What remains is a way to manage these things together in an IoT system that is scalable, secure, performance oriented and interoperablewhich complies with the standards.*

Industrial Internet of Things, IIoTwill have an impact on the legal, ethical, security and social fields. Workers could potentially abuse it, hackers could potentially access it, corporations may not want to share their data, and individual people may not like the complete absence of privacy.

For these reasons, the Internet of Things especially IIoT needs to be better managed, better planned and better designed. This needs to be done whilst ensuring a secure and seamless data flow between the devices and cloud.

Our analysis also conclude that most of the aforementioned challenges can be tackled, various uses cases can be solved using smart tools like Winjit's IoT Sense, Azure IoT Hub, and Secure IoT Sensors.

Ultimately, Rapid solution development  withcognizant engagement, discussion, and collaboration across varied stakeholdersis the most effective way forward.

# References


1. http://www.cisco.com/c/en/us/solutions/collateral/enterprise/-cisco-on-cisco/Cisco_IT_Trends_IoE_Is_the_New_Economy.html
2. http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.asp
3. http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf
4. http://www.cmo.com/features/articles/2015/4/13/mind-blowing-stats-internet-of-things-iot.html
5. http://www.ti.com/lit/wp/spmy013/spmy013.pdf
6. https://www.internetsociety.org/sites/default/iles/ISOC-IoT-Overview-20151221-en.pdf
7. http://www.huawei.com/minisite/gci/en/index.html
8. https://www.prokarma.com/blog/2015/02/17/iot-gateways-way-iot-networking