Survey on IoT for Challenges and Technical Solutions

Dipak S. Shirsode **Akshay S. Nakshane** **Pranoti R. Patil** **Prof. Dhiraj D. Shirbhate**

Abstract — **Results to cope with these challenges Using internet of things (IoT) to connect things, service, and public for intelligent operations has been discussed and deployed in many industry domains such as smart energy, smart city, healthcare, food and water tracking, logistics and retail, and transportation. However, scarce information is available for IoT usage in industrial automation domain for reliable and collaborative automation with respect to e.g., enabling scalable collaboration between heterogeneous devices and systems, offering predictable and fault-tolerant real-time closed-loop control, and inclusion of intelligent service features from edge devices to the cloud. In this paper, clarify the specific quality attribute constraints within industrial automation, present specific industrial IoT challenges due to these constraints, and discuss the potentials of utilizing some technical.**

Key Words — **Internet of Things, Security Challenges, Industrial Automation Challenges.**

I. INTRODUCTION

IOT means internet of things it is the method of connecting the object or the things through wireless connectivity. The IoT is "a self-configuring and adaptive system consisting of networks of sensor sand smart objects whose purpose is to interconnect all things, including every day and industrial objects, in such a way as to make them intelligent, programmable and more capable of interacting with humans". The IoT extends the cloud computing concept beyond computing and communication to include everything, such as physical devices.

Industrial internet uses sensors, software, machine-to-machine collaboration and different technologies to gather and analyze data from physical and virtual world for optimized operations and providing services. In the mean while, trends such as fast-changing and changeable market needs and customer requirements, the customer expectation of responsiveness, and the connectivity capability becoming available to embedded systems are triggering many companies to move from products to services, and continuously deploy new features that increase the capabilities of existing products to create new business opportunities.

Accordingly, many organizations start to evaluate IoT as a potential value creator in their business strategies, through the combination of advanced data analytics and IoT to connect machines, computers and people to enable intelligent industrial operations in many industries, such as industrial domain, smart city domain, and health well-being domain.

Electronics, sensors, and network connectivity, are those things are connected with the IoT network of physical object. When everything is connected, increased efficiency is possible and improved communication allows access to data where and when it can best be used. Machines can communicate directly by machine-to-machine interfaces and factory data can be made available to customers. Industrial computers become the heart of this revolution, storage, handling data processing, connectivity and interfaces. For instance, remote location of plants would benefit from technologies that support remote operation.

Industrial automation is a domain in which IoT can bring with various benefits. For instance, remote location of plants would benefit from technologies that support remote operation as well as maintenance; autonomous collaboration between devices so that devices are aware of each other for information exchange, in this way to decrease engineering costs in terms of manual configurations of all involved devices; the real-time data collected from a large number of these interconnected physical hardware units can be used for developing new intelligent applications, etc. The main purpose of this report is therefore to identify these challenges, within industrial automation domain in particular, and discuss how some potential technologies can be deployed to face with these challenges.

II. LITERATURE REVIEW

The revolution of the Internet was the catalyst that changed the future of communication forever. the transfer of information is allowed for despite the geological barriers that separate the computers. As time has progressed, developed new technologies that have allowed us to move from the1st generation of the Internet into the current transition into the 4th generation. This generation has been propelled by the concept of the IoT. Currently, the Internet is able to collect data on each individual that accesses it. IoT is a technology that deals with bringing control of physical devices over the internet. This is propose efficient industry automation system that allows user to efficiently control industry appliances / machines over the internet.[1]

IoT is the network of physical objects (things) embedded with electronic software, sensors, and network connectivity which enables these objects to collect and exchange data. In this paper, developing a system which will automatically monitor the industrial applications and generate Alerts-

Alarms or take intelligent decisions using the concept of IoT. Hence IoT is rapidly increasing technology.[2]

The IoT is networks of physical object that contain embedded technology essence communicate with extrinsic environment. The IoT is part of internet that focuses on devices and object used in business setting. It helps to connect to the internet including wearable devices, metering devices and environmental sensor. These devices will connect to internet to share different types of data. This is proposed Industrial Automation using cloud computing and sensing based applications for IoT. In these paper the sensing device is used to check different behavior like fire, humidity, temperature of room.[3]

III. INTERNET –OF- THINGS FOR INDUSTRY

The purpose of the IoT to the developed industry is called the IIoT(Industrial Internet).The IIoT is part of a superior concept known as the Internet of Things (IoT). The IoT is a network of intellectual computers, devices, and objects that collect and share massive amounts of data. The collected data is sent to a central Cloud-based service where it is aggregated with other data and then shared with end users in a useful way. The IoT will increase automation in homes, schools, stores, and in many industries.

The domains and use cases for which most prospective IoT intelligent solutions are being designed or implemented cover smart cities, smart energy and smart grid, healthcare, food and water tracking, logistics and retail, transportation. Within industrial domain, most IoT applications address logistic and product lifetime management, agriculture and breeding, and industrial processes, in which assets analytical is a key application Therefore, flexible and cooperative automation needs a holistic industrial IoT solution that addresses business, technologies, and architectures aspects in order to provide real-time closed-loop control for optimization and improved uptime enable horizontal relationship between devices, and offer secure and expected inclusion of service features vertically from edge devices to the cloud.

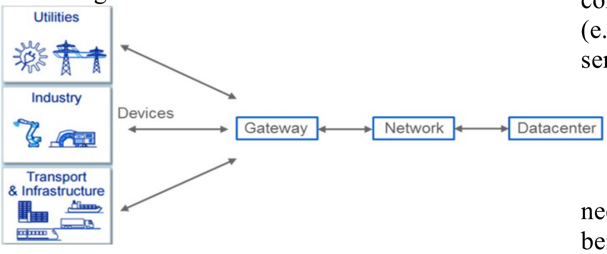

Figure 3.1:- Industrial IoT from Edge to Cloud

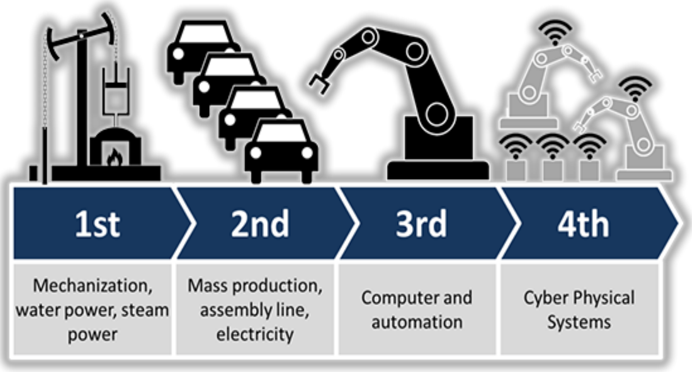
1st
2nd
3rd
4th
Mechanization, water power, steam power
Mass production, assembly line, electricity
Computer and automation
Cyber Physical Systems

Figure 3.2 :- Industrial Revolution

IV. IoT Challenges in Industrial Automation

Consumer and Industrial IoT have correspondence in many senses, though there are key differences that are reflected in specific real-time and deterministic requirements of industrial IoT applications as well as severity of consequences if breakdown occurs in the industrial IoT applications where perfect operation is expected due to the more investment in capital. In this, 1st we will describe general IoT challenges. Then it will describe the main quality feature constraints within industrial automation, and discuss specific industrial IoT challenges due to these constraints.

1. General IoT Challenges

-

ata and service security

Major applications and services based on IoT are increasingly at risk to trouble from attack or information theft because having more devices, systems, and technologies connected leads to more decentralized entry points for these security trouble. As unavailability of service or data can have severe impact on the customer businesses, it is important to provide security platform to increase the level of data fortification and security for messages communication between devices as well as from devices (e.g., sensors, actuators, etc.) to the cloud platform to ensure service continuity and required Quality-of-Service (QoS).

- **Trust, data integrity and information privacy**

The interconnected devices and the users of the system need to have assurance that the information and services being exchanged can be dependable. Therefore, trust mechanisms need to be able to deal with humans and machines to ensure truthful access to data and proper authorization of service.

- **Scalability**

This challenge is reflected in different aspects including:

i. Naming and Addressing – the scalability of the device address of the existing network must be sustainable;

ii. Data communication and networking – the connection of new networks and devices should not risk the performance of existing networks, devices, and data transmission even though the high level of interconnection among a large number of devices .

- **Interoperability**

Industry is dominated by proprietary interfaces and solutions. The amount of devices and system components from different seller and different domains poses challenges in terms of multiple platforms, several protocols and large numbers of APIs. According to , the vast multiplicity of devices, applications, and implementations within the industrial IoT will result in a extremely heterogeneous set of data with variation in format and analysis of data, quality, frequency, and timing of the data.

2. Automation Domain-Specific Constraints

Industrial automation spans over many different types of control systems, e.g., motion control, protection systems, and digital control.

- **Timing and determinism**

Industrial control systems are real-time systems that have strict requirements on the system's chronological behavior, accuracy, and response. A existing example is a control system for industrial robots in the context of welding, where sensors need to detect the position and direction of seams, the signals from sensors have to be processed rapidly to enable the robot controller to change the direction of motion in time. The accuracy requirement for the industrial robots are related to the timing requirements for the services involved, e.g., sampling a measurement at precise and deterministic intervals. For these industrial control systems, there are also timing interactions involved in different processes that are executed in the system.

Reliability and availability

The main indicators for reliability and availability include (i) Mean Time Between Failure (MTBF), which is usually a statistical demonstration of the likelihood of a component, device, or system to fail; (ii) Mean Time To Repair (MTTR), which is the average time to repair a system, or component, that has been unsuccessful.

- **Safety and criticality**

From a functional safety perspective, it is difficult to use software technologies (such as operating systems) that are developed for general purpose in a safety context, e.g., protection functionality that puts the system into a safe state in case of an fault.

- **Interoperability**

A typical industrial process control system consists of thousands of components including a network of many workstations, servers, controllers, and up to several hundred thousands of individual I/O signals from various devices. There is thus a huge challenge in managing the large diversity of components from different manufacturers.

V. Industrial IoT Challenges

1. Mixed criticality

A lot of functions are integrated in an industrial automation system. These functions are of different criticalities dealing with controller compute logics, real-time and non-real-time functionality, and protection. As accessibility and reliability are given more and more precedence in many products, systems, and services, these functions of different criticalities need to be separated so that functions of low criticalities would not interfere with a high-criticality function.

2. Latency

With hundreds of thousands of sensors, actuators, programmable logic controllers connected, it is important to have consistent and deterministic data transfer and analysis in real time. Due to the use of internet connections and wireless connections for industrial IoT solutions, the assumption about the certainty of the network latencies of industrial control system in Local Area Network (LAN) environment has changed. According to, the internet roundtrip delay ranges from tens to a few hundreds of milliseconds.

3. Fault tolerance

To ensure industrial constraints on availability and reliability, it is important to consider how to design fault-tolerant systems to be adaptive to unpredicted events like failure of underlying services, malicious attacks, or changes in the quality of particular services, as well as faults that are related to internet communications and cloud software technologies when providing real time services.

4. Scalability

Many industrial plants could have tens of thousands of control loops and applications to maintain the desired performance in operation. These different industrial control applications have different cycle-time requirements.. This implies huge amount of data that need to be managed through e.g., filtering, pre-processing at or close to edge devices before sending to the cloud.

5. Functional safety

Functional safety is critical for the overall safety of a system or product that depends on the correct implementation of specific commands and functions. The oil and gas industry, nuclear plants, etc. all rely on functional safety that offers the necessary danger reduction required to achieve safety for the tools. Safety function and safety reliability are two types of requirements to achieve functional safety . The safety concern is reflected in both hardware and software within process industries, which insist close integration of safety and control applications such as emergency shutdown systems, fire and gas systems, which are Safety Integrity Level (SIL) compliant application solutions that prevent inadvertent/accidental control actions and provide added consistency and up time for the concerned processes.

6. Industry-specific security challenge

Industrial control systems often assume that the network in which they operate are (physically) secure and separated from outside interference. However, the introduction of IoT solutions that connect industrial machine sensors, actuators, and industrial networks poses a challenge that the data collected from these industrial devices and systems need to be stored in a secure and proper manner.

VI. Managing Industrial IoT Challenges

1. Managing Latency and Scalability of Data Through Localization of Computation

The term "fog computing" or "edge computing" pushes application logic and the underlying data processing from corporate data centers to the edge of the network. Running applications at the edge cuts down network latency and produces faster responses to end-users. Therefore, the fog/edge computing further extends the cloud computing by addressing real-time applications that do not fit the example of the cloud at the edge of the network, e.g., applications that require very low and predictable latency, and distributed control systems. These applications are hosted at the network edge or end devices to reduce service latency and improve quality of service (QoS).

According to Fog Computing supports emerging Internet of Everything (IoE) applications that demand real time/predictable latency, such as industrial automation domain, transportation, networks of sensors and actuators, and is suitable for real time big data and real time analytics. Besides the concept of edge computing, computation off loading is another way to manage latency by sending heavy computation to resourceful servers and receiving results from these servers, base don the available resources, such as network bandwidth, storage capacity, and processor performance. Several other studies address latency and data scalability issues as well.

2. Managing Mixed Criticality through System Partitioning

To enable software with mixed criticality to be co-existing in one device, virtualization is a technology that has gained increasing interest in industrial systems. Virtualization has been used extensively to manage resources in server based systems and it is a technology that is also starting to be applied for embedded real-time systems, with several commercially available products. In virtualization technology a virtual machine monitor or hypervisor manages how physical resources, like RAM memory, CPU, and network interfaces, are shared among a number of virtual machines (i.e., software partitions). Each virtual machine can run its own operating system independent of other virtual machines. Thus, it is possible to mix different operating system on a multi-core platform, and offer a high degree of independence between them. The ability to mix operating systems and to strictly separate different software partitions provides an opportunity to manage both legacy software running a traditional real-time operating system and new IoT related functionality of different criticality running on general purpose operating systems.

3. Managing Scalable and Secure Real-time Collaboration

Decreasing the engineering effort spent on complicated manual configurations of connected devices is essential for a scalable collaboration. Zero-configuration networking is a technology that allows communication between devices and improves network ease-of-use.

It is built on top of three core technologies,

- Link-local addressing – assigning numeric network addresses for devices in the network;
- Multicast DNS name resolution – automatic distribution of computer hostnames;
- DNS service discovery – automatic location of network services such as printers, cameras, speakers, gateways, etc.

4. Managing Fault Tolerance

There are different ways for achieving fault tolerance requirements. Redundancy in the system is one of the common design principle to use. Redundancy schemes include duplicating servers, controllers, I/O, and networks. For designs a distributed fault tolerance system that is run asynchronously by all redundant controllers. Also There are specialized controllers that offer built-in redundancy by applying dual processor modules that are synchronized at hardware level.

5. Managing functional safety

Functional safety in industrial systems has specific requirements and is governed by standards of safety and authority regulations. We see ,there are three different strategies for functional safety in an industrial IoT context; A 1st possible strategy is to completely separate the safety related systems from the IoT systems, which means that the IoT system is agnostic about the existence of any safety-related system. A 2nd approach is partial integration where information from safety related systems are isolated and do not depend on IoT systems but can provide IoT systems with information. Finally, 3rd strategy, theoretically, it would be to use IoT solutions directly for realizing safety-related systems, which might be in conflict with standards and regulations and thus require additional certifications within the foreseeable future.

VII. Advantages and Disadvantages

- **Advantages**

1. It improves worker safety.
2. It will increase operational efficiency.
3. It also increases productivity.
4. There are new opportunities for the business.
5. It Reduce downtime (IoT).
6. We get better understanding for customer demand.

- **Disadvantages**

1. **Compatibility**: There is no standard for tagging and monitoring with sensors. A uniform concept like the USB or Bluetooth is required which should not be that difficult to do.
2. **Complexity**: There can be much opportunities for failure with complex systems.
3. **Privacy/Security**: Privacy is a big issue with IoT. All the data must be encrypted so that data about your financial status or how much milk you consume isn't common knowledge at the work place or with your friends.
4. **Safety**: There is a chance of hacking, the software can be hacked and your personal information will misuse.

VIII. Application

Smart dust

The small sensor like as grain of sand, with the ability to sense everything from chemicals to vibrations, was first thinking up in the early-1990s, but little progress was made in the following years moving this interesting idea into a reality. However, interest in this hopeful technology has grown recently, Gartner predict smart particle will trend in the next six to eight years. In oil exploration companies spreading smart dust to monitor rock movements to small sensors all over factory equipment continually looking out for changes and problems.

Drones

Drones, Unmanned aerial vehicles have becomes one of the most talked about products in the tech space, thanks to their many useful application. the future of this machines play the main part in the IOT by action as either a sensor or by providing a relationship between sensors and data gathering points. Drones may not be seen as fully fledged connected IIoT device, but they can carry with all range of sensors and are autonomous machines capable of gathering massive amounts of valuable data. Construction companies can use drones to undertake daily land surveys and feed this data into software to ensure construction is on schedule and send an alert if anything looks out of place or improperly built.

Futuristic Farming

Far from the factory floor, in countless farms around the world, is where the IIoT could make the biggest dissimilarity. Utilizing the latest technologies is not anything new to the agriculture industry, but implementing smart, connected IIoT projects enables farmers to make use of the massive amounts of data generated on their company. The huge size of the farms makes manual surveys unproductive and tricky, most important farmers to turn to IIoT solutions. Oyster farmer Ward Aqua farms, with the telecoms firm Verizon, deployed an IIoT program to make the most of productivity and ensure the quality of food in the supply chain, using satellite imaging and IIoT track-and-trace technology to check farming operations all the method from harvest to delivery.

Aerospace

Aerospace companies have mainly introduced IIoT solutions on the factory floor for tracking tools and parts, with some beginning to expand the number of on-board IoT devices. An aero plane that knows when it's going to encounter maintenance problems before they actually happen would save a significant amount of man-hours and money for air lines.

Taleris, a joint venture by General Electric and Accenture, is at the forefront of developing IoT solutions for airlines, aimed at minimizing delays and disruptions by analyzing data collected from sensors on aero planes.

Energy Networks

Energy companies can expect to see their operations fundamentally altered when IoT is fully embraced in their sector. Spikes in energy consumption around major TV broadcasts and weather events have long troubled utility firms. But with effective energy demand management through the IIoT, the need for investment in both energy networks and power plants is reduced.

Smart meters are one example of the industry's move towards IoT technologies, although at the moment they only record usage amounts and timings. Utility firms could potentially provide price information to these meters, which could in turn interact with other IoT devices to use energy at the most efficient time.

IX. CONCLUSION

Now these time we need everything computerized. Earlier we can only examine the situations with the help of cameras. Internet of Things (IoT) is used for to reduce manual overhead in industry to monitor as well as to inform the responsible people to take proper measures, but this will partially complete our necessity.

It has the potential to change spending investment on building, maintaining, and upgrading infrastructures for multiple connected products. Through delivering software services for customer that are based on information extracted from multiple connected products, IoT provides a new way of realizing business alertness and faster innovation. Challenges within long lived industrial automation systems with huge complexity and proprietary solutions. By introducing industrial IoT, we can connect different long-live systems, and create new services based on fastest technologies, innovative IoT solutions will arise – this has so far been largely unaddressed by the Industrial IoT community, and remains to be a future research direction. IoT innovations is used in many industries such as smart city, smart energy, healthcare, logistics and retail, transportation, etc.

ACKNOWLEDGEMENT

The making of the paper needed co-operation and guidance of a number of people. I therefore consider it my prime duty to thank all those who had helped me through their venture. It is my immense pleasure to express my gratitude to Prof. D.D.SHIRBHATE as guide who provided me constructive and positive feedback during the preparation of this paper I express my sincere thank to the head of department Prof. J. H. SATURWAR and all other staff members of CSE department for their kind co-operation. I would like to thank Dr. A. W. KOLHATKAR, Principal of our institution for providing necessary facility during the period of working on this report. I am thankful to my friends and library staff members whose encouragement and suggestion helped me to complete my paper.

References:

1) Amruta P Bauskar, A Review on Industrial Automation Using IOT, International Research Journal, Volume: 03 Issue: 12 | Dec -2016
2) Ashwini Deshpande Industrial Automation using Internet of Things, International Journal of Advanced Research, Volume 5 Issue 2, February 2016
3) Geetesh Chaudhari, Industrial Automation using Sensing based Applications for Internet of Things, International Advanced Research Journal, Vol. 3, Issue 3, March 2016
4) B. Sosinsky, Cloud Computing Bible, ISBN 978-0-470-90356-8, Wiley Publishing, Inc., 2011.
5) S. Trujillo, A., Crespo, and A., Alonso, MultiPARTES: Multicore Virtualization for Mixed-Criticality Systems, Euromicro Conference on Digital System Design, 2013.

AUTHOR'S PROFILE

	Pranoti R. Patil BE CSE J.D.I.E.T YAVATMAL Research work 1on DATA MINING TECHNIQUES FOR FRAUD DETECTION
	Dipak S. Shirsode BE CSE J.D.I.E.T. YAVATMAL Research work 1 on DATA MINING TECHNIQUES FOR FRAUD DETECTION
	Prof. Dhiraj D. Shirbhate Asst. Prof. J.D.I.E.T YAVATMAL ME CSE ,Publications 10 on Database Research work 4 paper.
	Akshay S. Nakshane BE CSE J.D.I.E.T YAVATMAL Research work 1 on DATA MINING TECHNIQUES FOR FRAUD DETECTION