IoT beyond platforms

Enabling innovation at scale

wipro

Ecosystem-enabled growth, the key promise of IoT stems from the ubiquitous nature of the technology—its ability to cut across service components, including systems, processes, data and applications. While this ecosystem play of technologies, systems and organizations is what drives unprecedented efficiencies and innovation, no single platform can encompass the length and breadth of IoT. While there are a variety of platforms that can handle device integration, aggregation, presentation, monitoring, controls and analytics, what is needed is a holistic and integrated approach to IoT implementation.

Six pillars of an IoT implementation

Here are six critical elements that organizations must focus on to drive the success of IoT solutions and outcomes.

1 **Device:** High-level architecture of an IoT solution comprises two broad categories of devices—a) Gateway-like devices that aggregate and store data or route it to the cloud servers and b) Constrained devices (sensors, actuators, and controllers) that address a specific application function. By 2020, the installed base of IoT connected devices is expected to soar—while Gartner puts the number at 26 billion globally[1], Statista says it will touch 31 billion[2]. Unsurprisingly, this vast range cutting across industry segments adds to challenges in IoT solutions, given the lack of standards and various protocols of devices. Take, for instance, smart homes. While over 13% of consumers today own one or more smart home devices, IoT interoperability is a significant concern that prevents them from deriving ROI, heightened convenience or a smarter experience from these solutions[3]. This means driving sustainable IoT solutions requires businesses to focus on device integration and lifecycle management.

2 **Connectivity:** Platform connectivity plays a significant role in enabling real-time data flow—a critical element for IoT solutions. According to a survey of over 100 global transport and logistics companies by Inmarsat, 40% of respondents identified connectivity issues as one of the most significant challenges facing their IoT deployments[4]. IoT connectivity requirements have resulted in the evolution of IoT specific network solutions, besides standard IP and wireless networks. For instance, LoRa—the long range, low power wireless platform—is better suited for large enterprises where it is necessary to converge multiple solutions into a single communications backbone. Sigfox, a leading IoT connectivity service is ideal for a more comprehensive spread, such as that required in transport solutions. NarrowBand IoT (NB-IoT) focuses specifically on indoor coverage, low cost, long battery life, and enables a large number of connected devices. While these and other connectivity options have their merits regarding range, coverage, penetration, cost and power requirement, they are also fraught with challenges that need to be addressed holistically. Ensuring availability of devices and platforms that support these networks is therefore, a critical first step.

3 **Security:** With many new nodes being added to networks and intelligence shifting increasingly to the edge, IoT devices with their minimal device-level protection and ample security holes provide innumerable opportunities to hackers. In what is termed as a watershed moment in the European and U.S internet space, Dyn the company that controls much of the internet's DNS infrastructure, recently suffered a DDoS attack that brought down several sites, including Twitter, the Guardian, Netflix, Reddit, and CNN.

[1]Firstpost, Internet of Things Installed Base Will Grow to 26 Bn Units by 2020, https://www.firstpost.com/biztech/internet-of-things-installed-base-will-grow-to-26-bn-units-by-2020-1895781.html

[2]Statista, IoT Connected Devices Installed Base from 2015 to 2020 in Billions, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3]Techcrunch, Smart Home Technology Must Work Harder to Create Smarter Consumers, https://techcrunch.com/2016/05/14/smart-home-technology-must-work-harder-to-create-smarter-consumers/

[4]IoT Network News, Connectivity Challenges Threaten to Derail Logistics Sectors' IoT Efforts, http://iot-nn.com/2017/12/07/connectivity-challenges-threaten-to-derail-logistics-sectors-iot-efforts-says-inmarsat/

While datacenter level security is one aspect, securing devices at the gateway level or the edge is another critical aspect, which should be reinforced by device manufacturers.

In the aftermath of the attack, 14,000 internet domains, which accounted for approximately 8% of Dyn's revenues, dropped Dyn as their DNS service provider. Dyn confirmed that Mirai botnet, which largely comprises IoT devices such as digital cameras and DVR players, was responsible for the attack. While datacenter level security is one aspect, securing devices at the gateway level or the edge is another critical aspect, which should be reinforced by device manufacturers. Intelligent IoT gateways and multi-factor authentication must be used to safeguard communication between connected things and the cloud service, to maintain integrity, authenticity and confidentiality.

4 **Quality control and testing:** QA strategy is a major concern area in the IoT world—a collaborative space with several small and large contributors. Test labs, testing tools, simulators and emulators, along with testing methodologies and processes define the level of reliability, dependability, and risk appetite of the IoT solution. Two major areas of testing include the data interaction layer and user interaction layer, besides the platform's internal intricacies. Enterprises entering the IoT arena must ensure that the data interaction layer validates conformance to standards, interoperability and security, while the user interaction layer focuses on network capability, usability, and user experience. Recently, there was widespread outrage over Amazon's Echo devices—the company's IoT-enabled smart home automation devices that were accidentally set off by Alexa, Amazon's digital assistant and self-ordered unwanted merchandise. Alexa's voice recognition system is not tested to identify whether the speaker is an authorized user.

5 **Processes and standards:** Even as data is being collected every second from billions of IoT devices, regulatory authorities are still unclear on how to fully secure it for consumers, businesses, and governments. Currently, most companies are adopting the self-regulating policy when it comes to IoT solutions and while some have mature process and regulatory frameworks, others do not, creating widespread inconsistencies. Diverse groups such as the International Standards Organization, Underwriters Laboratory, ATIS, IEEE and 3rd Generation Partnership Project (3GPP), are currently working collaboratively to address IoT's regulatory issues[7]. Setting up processes

[5]The Guardian, DDoS Attack That Disrupted Internet was Largest of Its Kind in History, Say Experts, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[6]Gizmodo, TV Report on Accidental Amazon Orders Triggers Attempted Amazon Orders Across San Diego, https://gizmodo.com/tv-report-on-accidental-amazon-orders-triggers-attempte-1790958217

that do not hamper innovation in the IoT ecosystem requires a shift from fixed processes to frameworks that afford flexibility while adhering to standards.

6 **Managed services:** The real premise of IoT lies in deriving sustained benefits from its solutions at a larger scale, not just from pilot projects and POCs. This demands an effective service framework around IoT solutions to ensure smooth functioning of solutions, with sustained outcomes and continuous improvement in processes as well as solutions. Think about how ITSM and the emergence of 'Managed Services' concept transformed the IT world. Proactive processes and procedures are now used to plan, design, deliver, and control IT service delivery to business users. The IoT world needs an evolved version of ITSM to manage its ever-increasing number of connected nodes and data points. The good news is the IoT managed services market is expected to grow at a CAGR of 15.3% from 2016-2022[8].

IoT projects are sprouting like mushrooms, but how do you make them sustainable?

IoT projects have an alarming failure rate of 75%—failure to make the cut with cyber security and lack of experience being the two principal reasons contributing to it[9]. In most cases, IoT solutions are designed to solve specific business problems, leading to organizations dealing with a multitude of solutions from multiple vendors that are neither interoperable nor secure, and result in increasing complexity and costs.

IoT should be able to connect new and old systems together to drive results, making data aggregation and control crucial aspects. Unfortunately, these aspects are often ignored in favor of presentation and analytics. Most IoT devices fail to have a neutral data aggregation layer or have limitations regarding data formats or types of devices that can be integrated, making device manufacturing or proprietary play a significant reason for failure. Another frequently ignored aspect is applying 'controls' or insights to business decisions for superior ROI.

All of this makes it imperative to deploy IoT platforms that have inbuilt control logic and management capabilities. What businesses need today is an all-encompassing IoT stack that can operate with multiple disparate sensors, vendors, applications and data interchanges to simplify, accelerate and sustain the promise of IoT innovation at scale.

[7]The Verge, The Internet of Things is Going to be a Legal Nightmare, https://www.theverge.com/2015/1/27/7921025/will-self-regulation-be-a-huge-problem-for-privacy-in-the-internet-of

[8]GlobeNewsWire, Worldwide IoT Managed Services Forecast, https://globenewswire.com/news-release/2016/08/02/860825/0/en/Worldwide-IoT-Managed-Services-Managed-Security-Services-Managed-Networks-Managed-Devices-Managed-Infrastructure-Services-Market-Drivers-Opportunities-Trends-and-Forecasts-2016-202.html

[9]ZDnet, Cisco: Most IoT projects are Failing Due to Lack of Experience and Security, http://www.zdnet.com/article/cisco-most-iot-projects-are-failing-due-to-lack-of-experience-and-security/

How the mining industry automation solutions cut across the six pillars of IoT implementation to drive superior value and outcomes

Mining automation—the greatest driver of innovation in the traditional industry, relies heavily on integrated IoT solutions to:

- Manage exchange of information across industrial devices and equipment, perform tasks and feed data into software systems including aspects based on additional sensor sets for requirements like worker safety.
- Improve connectivity to enable miners to automatically exchange and process data, with minimal human intervention, thereby enabling remote monitoring of mining operations. This demands specialized communication options looking at terrain and lack of availability of usual communication options like MPLS, GSM, 3G, etc.
- Improve security of assets and workers as IoT-enabled mining automation solutions can help optimize mine layout, vehicle paths, and monitor data from sensors and equipment in real time, to protect equipment as well as the people handling it.
- Move from predictive QA and testing to preventive maintenance that helps minimize downtime and equipment failures, enable accurate spare parts ordering and so on. Underground mines specially demand six sigma standards to ensure safety and security aspects besides operations.
- Standardize processes and develop new business models that are highly agile and responsive.
- Implement IoT Managed Services to gain end-to-end visibility and greater control over mining operations for superior business outcomes.

About the author

Ashish Khare
General Manager and Practice Head – IoT & Smart City at Wipro

Ashish heads the Smart City and IoT at Wipro Limited and plays a key role in consulting and solutioning for IoT and Smart City covering Integration, management and business operations. He also owns few IPs in same space and one of those won Innovation award by CII in 2017.

He has 25 years of experience with proven track record for customer centricity and passion for excellence. His current focus is on new technologies and solutions specially around IT-OT convergence. You can reach Ashish at **ashish.khare@wipro.com**

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at
info@wipro.com

IND/B&T/MAY-OCT2018