



EXPLORING THE FIELD WITH IOT

Internet of Things can potentially lead to an infrastructural makeover of any business for the better. But it has its fair share of complexities which problematize its deployment.

BY POOJA JAIN POOJA@ACCENTURE.COM/IDA.COM

It has been 20 years since the term 'Internet of Things' was first used by Kevin Ashton in 1999. It was in a presentation to Procter and Gamble that Ashton coined the term to talk about the use of RFID in the supply chain optimization. A decade later, the IOT came off marked 9th April as the World IoT Day, identifying IoT as a force to reckon with.

Today in 2019, IoT is nothing short of a revolutionary technology that holds the power to transform the business right to its core. What began with Digital Transformation pervading all levels of organizations, from the factory floors to supply chain, to the top-most managerial levels, has now led the industry to a point where it is ready to integrate all these individuality technologically empowered operations into one giant spider's web.

Talking about the technological trends that have made IoT a possibility, Asoke K. Laha, President and CEO, Interra Information Technologies, says "Some of the trends that we are seeing include AI, social, legal, ethical IoT, Interomics and Data Breking, the shift from Intelligent Edge to Intelligent Mesh, IoT Governance, Secure Innovation, Trusted Hardware and Operating

System, Novel IoT User Experience, Silicon Chip Innovation and New Wireless Networking Technologies for IoT."

IoT Integrates Data.

The whole point of IoT is to connect all devices to ensure easy accessibility, operability and management. What in the hands of the end users is unmeasurable coexistence becomes a matter of

business value in the context of the enterprise. For the business, IoT signifies a convergence of the digital and the physical world. The first step is to connect all the devices and machines that a business uses – the physical resources and translate that to digital resources by pulling out data from them. IoT thus becomes a way for an organization to generate massive amounts



ABHISHEK RUNGTA
FOUNDER AND CEO, INTERRA NET TECHNOLOGIES

"The fundamental security weakness of the IoT Things is that it increases the number of devices behind the network's firewall. More than securing the actual devices, it takes more to secure IoT devices and it is also necessary to incorporate security into the software applications and network connections that link to those devices."



KAREN RAVINDRANATH
DIRECTOR - WEBNMS IOT (IOT DIVISION OF ZOHO CORP)

“The on set of IoT based Digital transformation across industries is a positive sign for increase in the IIoT adoption across enterprises. CIOs and technology leaders have to keenly look into fortifying their operations with data driven synchronization of IT and OT.”

of data, something that all twenty first century technologies from Cloud to Artificial Intelligence converge around.

Today, Data is the focal point of all organizations. Be it customer data, employee information, companies' confidential formula or the performance records of the machines, Data holds the key for the success of any business. IoT collects the Data that is a crucial business asset, while Cloud helps the enterprise to store this data and the domain of cybersecurity keeps this data safe from potentially hackers or leaks, and evolving technologies like Artificial Intelligence and Machine Learning helps process the data. IoT then becomes, the foundational step that no business can afford to overlook if it has to survive in today's Data centric enterprise.

With IoT the business can leverage data at multiple levels. Businesses can make strategic decisions based on the actionable insights from the past data, use real time data to manage operations in the present and use Predictive Analytical techniques to plan the future course of actions based.

Commenting on this potential that IoT brings Karen Ravindranath, Director - WebNMS IoT says, “Continuous monitoring of processes and digitization of data allows easier Root Cause Analysis which when fed into AI and ML systems



JAGAT PAL SINGH
CTO, CYBAGE

“Data strategy could be considered as one of the important aspects of IIoT applications. It can start from understanding how often data needs to be collected from the end points, to defining any metadata collection and data transformation needs before storing it.”

pick up from the room temperature and report that a particular machine needs to be looked at.

This brings about a shift from a reactive approach to a proactive approach. There is no longer the need to wait to be notified about a breakdown in order to take actions. By console management based on real time, the business can considerably reduce downtime and through that cut back the companies' losses.

Commenting on yet another potential use case, Neeraj Sharma, Country Head, UNSOC India, says “One of the biggest technological drivers of enterprise adoption of IIoT devices in India is the fast growing trend of digital payments. We are witnessing an exponential increase in the number of digital payments across the country, with the market expected to touch \$500 billion by 2020.”

IoT as a comprehensive re-modelling. The interconnected devices, machines and applications that IoT translates to, is not limited to costing operations within the department. But it allows the organization to bridge the gap between its different departments and have a unified front when it comes to the management of the business as a whole.

What this means is that, the immense Data that interconnected devices is bringing in for the business is open to being accessed throughout the organization. So, the logistics team can keep a track on the manufacturing process and coordinate their activities accordingly. This implies a confluence of information technology



NEERAJ SHARMA
COUNTRY HEAD, UNSOC INDIA

“A major challenge is the unpredictability of RoIs. The current level of IIoT technology demands heavy investments. And, yet, we don't have fully defined models of how those returns will be realised, because there is no historical point of reference.”

with operational technology in the industries. This results in unprecedented levels of operational visibility.

Explaining how IoT would impact everyday business operations, Karan Kumar, CTO Hogar Controls, says “IoT devices can help employers ensure worker safety and enhance overall workplace security. Using embedded sensors and wearables, workers in high risk environments like mining, heavy industries and construction can be continuously monitored and warned against falls and exhaustion. Small businesses can make use of connected video surveillance, cameras and smart locks to monitor office premises at all times and ensure the protection of important assets.”

Hence, the chain reaction that IoT sets off, leads the enterprise towards a highly transparent business model.

The other side of IoT. But this is just one side of the coin. Adoption of industrial IoT has its own shortcomings which the businesses cannot seem to get away from. The first being during the process of implementation itself. Because it requires them to overhaul the entire infrastructure or at the very least undertake some extensive upgradation.

Addressing this challenge, Jagat Pal Singh, CTO, Cybage, says, “Going up the organization



PREM RODRIGUES
DIRECTOR FOR SALES & MARKETING (INDIA, MIDDLE EAST & SAARC) - SIMON COMPANY

“Converged IoT system and devices delivers significant capital and operational savings and sustainability over the life of a facility through benefits like decreasing the number of disparate proprietary platforms, cutting power delivery cost per device, enhanced flexibility and less costly moves, etc.”

for IoT implementation can be challenging as CIOs will need to justify the costs and predict some ROI on the costs since IoT solutions and systems could turn out to be very costly upfront.” This means that making the business IoT friendly takes its toll on the overall budget. The fact that IoT brings with it an added vulnerability from the security point of view doesn't help its cause either. The interconnectivity that marks the foundation of IoT, inadvertently increases the risk quotient of the organization as there are now a larger number of devices serving as the entry point for the hackers to breach the firewalls of the company. IoT, through simplifying operations, also complicates security in the same step. There is no point in having massive amounts of data, if a company does not have the infrastructure to keep it secure from prying forces.

Another challenge that IoT poses, is the lack of a universal standards that govern the functions of IoT. Being a fairly new technology in the enterprise that has not yet to see a high scale adoption drive, IoT comes with a uncontrolled, unregulated playing fields, where each player in the market is free to make what they will of the technology without being governed by any standardizing authority. This kind of free reign that IoT enjoys, makes it both exciting and risky to be deployed. Lacking, because it is open to experimentation. All organizations can unrestrictedly push the boundaries of IoT as there are no prescribed guidelines to be followed. This unregulated exploration in to the uncharted territory simultaneously makes the business vulnerable to failure. If an organization can discover a new use case of IoT, they are equally likely to stumble upon a problematic, that can potentially compromise their business.

Finally, Therefore, businesses need to be extra careful about where they are heading with IoT. There is potential in the technology waiting to be harnessed, but if not handled with caution, it can also prove to be a rather risky venture. Abhishek Rungta, Founder and CEO, Indus Net Technologies gives a five steps guide to making an organization IoT friendly - 1) Create IoT adoption catalysts within the IT organization, 2) Build a sandbox infrastructure for innovation and experimentation, 3) Prioritize learning projects and pilots, 4) Get the infrastructure “IoT ready” and 5) Partner for success. Adoption of IoT poses challenges for the business at the levels of implementation, management and security. But once deployed well, it can prove to be a game changer for the organization.