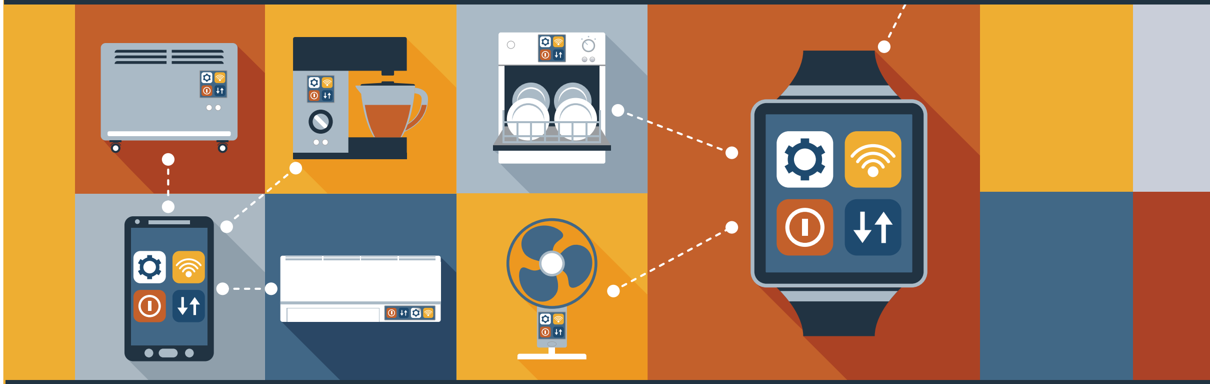
THOUGHT LEADERSHIP SERIES



Preparing for the INTERNET OF THINGS

database
TRENDS AND APPLICATIONS

ONE COMPLETE MARKETING PROGRAM

2016 | JAN

Eight Challenges From the INTERNET OF THINGS

THE INTERNET OF THINGS (IoT) may mean extended, real-time connectivity to many devices, opening up new avenues for intelligent products and services. However, for data executives, it also means new challenges not previously encountered in enterprises. Managing data—lately, known as "big data"—has always required a mix of technical and business skills. In the future, even big data as we've known it will swell exponentially as the IoT comes online. The business benefits from extracting and leveraging real-time, streaming data about people, products, and systems will be impressive. Data executives will need to adopt new ways of thinking and managing to ride the coming IoT wave.

Here are the eight key challenges that are shaping our IoT future:

1. MOST IOT DATA WILL REMAIN INACCESSIBLE FOR THE FORESEEABLE FUTURE

For starters, it will be a long time before enterprises will be able to fully tap into the increasingly rich vein of IoT data. There are countless devices, sensors, and systems that house data that is local, and will remain so for some time to come. The challenge will be to locate the data sources that are relevant to business requirements, and outfit these sources with network capabilities. Calculations from ABI Research estimate that the volume of data captured by IoT-connected devices exceeded 200 exabytes in 2014, and will grow to 1.6 zettabytes by 2020. However, the consultancy also estimates that more than 90% of IoT-generated data is stored or processed locally without a cloud element, rendering it inaccessible for analytics. The challenge is being able to surface this data for analytic purposes.

The good news is that it's getting easier every year to tap into these data sources. Remote tags and sensors have been in use for some time, and organizations have been collecting data from the field or point-of-sale locations. This data has typically been difficult to collect efficiently from remote locations and expensive to analyze in large quantities. The boom in wireless networks and connectivity is bringing accessibility to every corner of every enterprise and beyond. Plus, with the growth of cloud-based services, there are easy and cost-effective ways to store and manage this data. With the rise of open source data management tools and frameworks, it's now possible to process large volumes of this data for analysis cost-effectively as well.

2. IOT IS MORE THAN DEVICE DATA

IoT is typically associated with monitoring and collecting data from devices, including sensors, wearables, and mobile phones. However, organizations are looking to do more than simply monitor data. They see significant value in being able to get a clearer view of their markets and customer experiences to boost customer service, improve employee productivity, and better engage with partners. There are also benefits to be gained on a global scale in terms of greener uses of resources. A survey of early IoT adopters conducted by Verizon and *Harvard Business Review*, showed that many IoT initiatives are being driven by the need to improve customer service (51%), increase revenue from services and/or products (44%), improve use of field assets field (38%), and boost analytics (35%). The survey also found success so far in these efforts: 62% of respondents say IoT has increased customer responsiveness; 58% say it increased internal employee collaboration; and 54% have seen better market insights.

> *The greater volume of real-time data streaming in from all corners means that new classes of applications—and a new breed of analytical thinkers—will be required.*

3. IOT APPLICATIONS CREATE DIFFERENT VALUE IN DIFFERENT SETTINGS

IoT implementations—and the benefits realized—vary greatly from industry to industry. Manufacturing companies will see the greatest value from the start, according to a report by McKinsey Global Institute. Factories could realize potential value of up to $3.7 trillion by 2025, as machines, tools, and processes are tracked and analyzed.

For example, Airbus has launched a "Factory of the Future" initiative in which it intends to employ IoT technologies, along with smart machines and wearable augmented-reality devices to bring its systems together, and coordinate and share data. This will help manage the manufacturing and assembly processes for aircraft, which involves tens of thousands of steps that must be followed by operators, as well as for subassemblies that may have up to 400,000 points that need to be tightened down. Having these steps and tools online and digitized will save the manufacturer hundreds of thousands of dollars and ensure greater safety.

Additional business settings identified in the McKinsey study that will benefit from IoT include retail establishments, which will see value from automated checkout, layout optimization, smart CRM, in-store personalized promotions, and inventory shrinkage prevention; worksites, which will derive value from operations optimization, equipment maintenance, health and safety, and IoT-enabled R&D; and offices, where value will come from organizational redesign and worker monitoring, augmented reality for training, energy monitoring, and building security.

4. IOT BRINGS REAL-TIME INTO THE SPOTLIGHT.

Situational awareness—and the ability to react instantly to critical events as they happen—has long been sought by enterprises, and this is now possible with IoT. The challenge is to address the potential latency in sending data and application calls back and forth between devices and centralized systems. There are a range of systems that require real-time processing capabilities—from engine monitoring to onboard sensors to CRM applications extracting real-time mobile feeds.

5. IOT EXACERBATES SHORTAGES OF HARD-TO-FIND ANALYTICS SKILLS

The greater volume of real-time data streaming in from all corners requires new classes of applications—and a new breed of analytical thinkers. Individuals who possess the training in statistics and mathematics that is required to become a data scientist are few and far between. Data management teams will need additional skills training to expand their positions within enterprises—from more traditional roles of maintaining and securing data to storytelling and business analysis. Business users also need to be brought up-to-speed with data analysis techniques in order to fully understand and take advantage of IoT's business potential.

6. IOT SHIFTS THE EMPHASIS BACK TO HARDWARE

While the future belongs to the "software-defined" data center, taking advantage of IoT is a hardware concern, as it will require greater investment in low-cost, low-power hardware. Enabling and leveraging IoT may mean building, equipping, and maintaining far-flung IoT environments. At this point, IoT manufacturers tend to have their own standards and protocols, and thus, it's still up to enterprises to figure out how their networks of data sources and devices will all interconnect and communicate. Falling prices for commodity hardware pieces—such as RFID sensors and storage—will help ease the costs associated with building out an IoT-enabled system.

7. IOT CREATES MANY PRIVACY AND REGULATORY CONCERNS

The growth of IoT means a far greater distribution of data and movement through countless devices that fall beyond the control of enterprise administrators. Devices on the internet are easily hackable, as they tend not to be equipped with robust security software. There is also the matter of data ownership, which is not clear if data is streaming between devices and cloud sites.

8. IOT REQUIRES OPENING ORGANIZATIONAL SILOS

Moving forward into IoT means that relationships between organizations and their customers will change, as will relationships that are internal to organizations. For example, an engine equipped with on-board sensors that are constantly streaming data back to a manufacturer means that the manufacturer will need to remain in constant contact with customers to provide alerts when equipment failure is detected, or new upgrades are required. This will require that product technicians and designers work closely, perhaps even on a day-to-day basis, with sales account representatives or customer service departments. ■

—*Joe McKendrick*

Objectivity

Missing Link—The Criticality of Analyzing Relationships Within the Industrial Internet of Things

B2B APPLICATIONS FOR THE IOT, collectively known as the *Industrial* Internet of Things (IIoT), are receiving increasingly significant economic investment because of their projected impact on business and the economy. Experts predict that IIoT solutions will dramatically increase productivity and efficiency, and enable new business models that could transform entire industries. By 2025, the IIoT could have an economic impact of almost $11.1 trillion (McKinsey and Company, 2015).

While the possibilities of economic transformation are exciting, the IIoT remains in its infancy. Although early adopters in Manufacturing and Oil and Gas are already seeing returns from operational efficiencies and productivity, 88% of respondents to a recent World Economic Forum survey reported that they “still do not fully understand its [IIoT’s] underlying business models and longer-term implications for their industries.”

A critical technical challenge to implementing an IIoT solution is the ability to take action on sensor data in real time. Traditional database management systems are designed to run one-time queries over finite datasets. However, IIoT applications involve streaming data, such as network monitoring, financial analysis, logistics, and sensor network-based data. IIoT applications are relationship-analysis based applications that require long-running, or continuous, queries over unbounded streams of data. At the same time, these IIoT applications must reference non-streaming resources, such as historical data in databases and machine-learning models.

The common element among IIoT applications is the need to support relationship and pattern discovery. The ability to analyze the connections between data points is the missing link that transforms today’s typical Big Data stack into a system capable of delivering insights in real time. Solutions that enable relationship-based analytics are designed to integrate and organize data coming in from multiple sources in order to present a unified view of that data. However, it is very expensive, time-consuming, and technically challenging for an organization to build their own implementation.

To address this issue, Objectivity introduced ThingSpan, a purpose-built, integrated platform for deploying relationship analytics functionality within an IIoT application. ThingSpan supports pattern discovery by leveraging Hadoop with Apache Spark and supporting streaming messaging tools such as Kafka atop an object-oriented database designed for fusing data streams with non-streaming data sources. ThingSpan dramatically reduces the time, complexity, and cost of creating an IIoT application, enabling companies to achieve business insights from big data and real-time streaming data with high efficiency and at scale.

ThingSpan and relationship-based analytics have many critical use cases, including:

Utility Situational Analysis—Utilities organizations routinely collect and analyze data to make business decisions on how and where power should be distributed throughout their networks based on this analysis. The proliferation of smart meters and grid sensors, the rise of distributed generation resources like rooftop solar and behind-the-meter batteries, and the emergence of customers equipped with new technologies to manage and control their energy use are all bringing far more data under the purview of utilities than ever before. The sheer volume of this streaming data is already beyond the capacity of legacy data integration, management and analytic tools.

As a result, the ability to derive actionable insights from disparate data streams and sources in days versus weeks or months provides major competitive advantages. Systems that fuse streaming sensor data with transactional and historical data outside of traditional data warehouse and ETL tools are providing these benefits today in leading utilities companies, such as Pacific Gas & Electric and Florida Power & Light.

Logistics Asset Management—Logistics and transportation organizations, such as UPS, FedEx, Penske, and Con-way, have recognized the value of leveraging telemetric data from their logistical transports (cars, trucks, airplanes, etc.) to better manage routes and deploy more efficient predictive maintenance plans. For example, UPS has stated that the equivalent of saving 1 mile per driver per day results in savings of over $60 million per year.

In order to drive greater savings and productivity, these companies have heavily instrumented their transport vehicles to accelerate and improve their sensor-to-insight dataflow to drive better route and predictive maintenance systems. Leading organizations have deployed relationship analytics systems that fuse telemetric data (GPS, brake use, engine idle time) from their transportation fleet with historical, weather, traffic, customer inventory, geospatial (i.e., adverse terrains) and other transactional data.

These are just a few of the many use cases currently being evaluated by businesses around the world. Together, we expect to see these transformative technologies enable IIoT solutions that will revolutionize industries. ■

OBJECTIVITY, INC.
www.objectivity.com

VOLTDB

A Fast Data Architecture Is the Key to IoT Success

The Internet of Things, or IoT, is a notional distributed computing environment in which any sensor or device with an on/off switch can be connected to the Internet. There are a lot of these connected devices out there. Analyst firm Gartner forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015.

This global connectivity of devices and services is helping to bridge the gap between disparate systems to provide more insight, visibility and intelligence in everything from farming, utilities and home security, to public transportation.

A recent McKinsey report notes that IoT has the potential to represent nearly 11% of the world's economy by 2025, meaning that a well-developed IoT plan will be necessary for enterprises to derive a significant and positive impact from IoT—if the plan is implemented correctly.

The data gathered by IoT sensors and devices can help an enterprise to make informed decisions. However, the key to the effectiveness of these decisions is dependent on how quickly information is analyzed and understood in order to make the data useful and actionable. Knowing a power grid 700 miles away went down 10 minutes ago vs. 60 minutes ago, for example, is a big difference—and can create business value for the enterprise that gets there first.

When dealing with IoT there are usually five steps involved. First, the data is generated by a connected device, which is then passed over networks to a data storage solution. From there, the data is either manually or automatically analyzed. Depending on the results, alerts are sent to other devices (M2M), to the enterprise, or to people to take action.

The data generated from IoT devices is fast data, or data in motion. Fast data is the lifeblood of real-time businesses, which are defined by the speed of their operations. While there's a lot of media coverage and discussion about technology for big data and analytics, most of it focuses on historical data and has nothing to do with operations.

However, placing an operational database at the front end of your IoT data stream means understanding data instantly —and gives you the ability to act on it instantly. For example, energy companies are implementing smart metering solutions which allow utilities to capture energy consumption information in real time, enabling price-setting agencies to dynamically set different prices, based on usage patterns, time of day, and season. Smart meters also enable utilities to collect data at frequent intervals, analyze it, and make decisions in real-time to drive down energy usage.

One such company is deploying a smart metering solution based on VoltDB to process high-volume data streams of metering traffic, analyze the data quickly, and enable rapid, policy-based decisions formulated to reduce energy consumption.

Each utility customer is provided with an electricity budget, and the energy company leverages the fast data to alert them when their usage is trending toward exceeding the forecasted energy budget. These smart meters transmit power utilization data to the utility, and VoltDB's high-velocity data ingestion engine enables the utility to generate insights from the streams of incoming data on a per-event basis.

The energy provider can leverage the speed and real-time analytics of VoltDB to add context and intelligence to usage data as it arrives, automatically implementing actions to drive down energy consumption. The relational database combines the capabilities of an operational database, real-time analytics, and stream processing in one easy-to-use platform. With VoltDB, the utility leverages database-oriented applications against energy consumption data feeds to trigger alerts, validate meter operational status, and notify consumers and companies when planned consumption levels are being exceeded.

This is a real-life, in-production IoT solution. The electric company gathers data from 4.1 million meters using VoltDB for meter data management and billing. This intelligent solution allows utilities to process information from the smart meters using the data to automate actions based on defined policies.

For example, the reporting meters are automatically compared to identify meters that did not provide a current status. If a meter misses a defined number of consecutive reporting intervals, a technician is automatically assigned to fix or replace it. Similarly, if an unrealistic deviation in a meter usage pattern occurs, a technician is automatically assigned to inspect the meter in the field. Meters that report but are not yet registered in the system can be flagged so they can be reconciled to capture billing information.

By implementing the smart metering solution, utilities can build customer loyalty by leveraging fast data to help consumer and commercial customers reduce energy costs while more efficiently utilizing energy resources. ■

VoltDB
www.voltdb.com

Hewlett Packard Enterprise

Data-Centric Security for the Internet of Things

THE INTERNET OF THINGS (IOT) creates new, critical security challenges in the escalating fight against cyber-crime, in two key areas:

- Securing data from theft as it is generated, collected and analyzed
- Protecting IoT devices from potential use for physical attack

BIG DATA AND IOT—EXPANDED ECOSYSTEM EXPANDS SECURITY RISKS

As top use cases for data science/Big Data projects include real-time analytics for operational insights, and centralized data acquisition or staging for other systems, these projects can include massive quantities of sensitive payment card, personally identifiable and protected health information (PCI, PII and PHI). These projects alone hold major risk and now, with the advent of IoT, sensor data from devices adds to the sensitivity, risk factors and urgency.

The risk of data breach is high. The first step attackers take is to build a map laying out the network of the target organization to identify which systems are located where. Their goal is to set up mechanisms to acquire data over as long a run as possible and monetize it. When an enterprise builds a Big Data environment, the target has already done a lot of work for the attacker. With Big Data the enterprise has created a single collection location for the data assets the attackers are seeking.

While perimeter security is important, it is also increasingly insufficient. It takes, on average, over 200 days before a data breach is detected and fixed[1], leaving the most sensitive data assets exposed while attackers funnel data out of their target, with the scale of the breach growing every day.

With IoT connected devices, physical risk is added to the data breach risk. For example, there are Internet-connected devices that allow consumers to open and close the door to their homes from their cell phones. What prevents the attacker from doing the same thing? Imagine an HVAC system, gas appliance or medical device. If an attacker can control these systems, it becomes an attack on the individual, where the attacker can sit anywhere in the world. This is why everyone needs to be concerned about security in the IoT age.

With IoT devices there are multiple attack vectors such as impersonation of the device user, or of the service provider. These vectors can be protected against by the use of SSL technology, 2-factor authentication, and certificate pinning, so that SSL certificates only enable the device to connect to a server when the certificate matches certain criteria and can be trusted. IoT devices can be designed not to accept inbound connections directly, but rather to accept a request to "call me now" for connection to the genuine service provider. Device software security can be enabled through best practices in the application development process.

DATA-CENTRIC PROTECTION FROM THE DEVICE TO THE BIG DATA PLATFORM

To protect sensitive data assets, a new approach is needed—one that actually protects the data itself. Consider the most advanced payment security technologies to protect credit card data. Strong encryption is implemented inside the card reader to protect data as it enters this hardened device and before it ever gets to the Point-of-Sale (POS) terminal. Data passed from the card reader to the POS terminal is thus not usable by attackers.

A similar approach is needed in IoT. Since each device is different in terms of the data it collects and sends to the backend server, it is important to understand what data is sensitive. With that understood, it is a best practice to use data-centric, field-level encryption to protect individual data fields. This should be done through a special form of encryption referred to as Format-Preserving Encryption (FPE), implemented throughout the ecosystem—in the devices, the communications channels and the Big Data platform.

FPE is proven and in the process of being recognized by key standards bodies such as NIST (publication SP800-38G). It is a form of AES encryption that has been in use for some time—but unlike AES, which encrypts data into a large block of random numbers and letters, FPE encrypts the original value into something that looks like the original, so that, for example, a credit card number still looks like a credit card number. Sub-fields can be preserved so that the inherent value of this information can be maintained for analytical purposes. Analytics can almost always be done with the protected data, securing sensitive data from both insider risk and external attack.

CONCLUSION

The Internet of Things, with double-digit growth and billions of devices, creates great new opportunities but also new levels of risk for companies and consumers. Traditional security measures alone are not enough. Enterprises implementing IoT strategies need to apply a data-centric security solution end-to-end from the big data platform to the IoT infrastructure. Using FPE to encrypt data values on a field level, from the device to the infrastructure and remote control element, removes risk and enables protection against remote takeover of an IoT device—the biggest threat to IoT security. ■

HPE SECURITY – DATA SECURITY
www.voltage.com

[1] "Improve your data security and keep the hackers out"—Dick Bussiere, Tenable Network Security http://intheblack.com/articles/2015/06/01/improve-your-data-security-and-keep-the-hackers-out