The Internet of Things

Linkages to Software Engineering

CSCI 510 – Software Engineering Economics, Professor Barry Boehm
USC Viterbi School of Engineering Center for Systems and Software Engineering, November 28, 2018
Personal Information

Len Cayetano

✓ Senior Software Development Manager, Zetron Inc.
✓ 20 Plus Years in Software Engineering
✓ Double Alumnus, University of Southern California
  ❖ MS Software Engineering, Viterbi School of Engineering
  ❖ MBA International Business, Marshall School of Business
✓ Loyola Marymount University, Los Angeles
  ❖ MS Computer Science
✓ DePaul University, Chicago
  ❖ BS, Dual Major in Mathematics & Computer Science with Honors
✓ Email: lcayetano@alumni.usc.edu
Learning Objectives

Objective 1
Increase Awareness of Important Trends in Technology

Objective 2
Appreciate Intrinsic Linkage Between Innovation and Software Engineering

Objective 3
Leverage concepts and Principles of Software Engineering Economics

Objective 4
Reinforce Importance of the Incremental Commitment Model

Objective 5
Gain Insights into IoT
Current Technology Trends
Gartner Top 10 Strategic Technology Trends for 2019

Empowered Edge
✓ Cloud services will be managed as a centralized service executing on:
  ✓ Centralized servers
  ✓ Distributed servers on-premises
  ✓ On the edge devices themselves

AI-Driven Development
✓ Developers will have an ecosystem of AI algorithms and models
✓ Development tools will be tailored to integrate AI capabilities and models into a solution

Autonomous Things
✓ Robots
✓ Drones
✓ Autonomous Cars

Digital Twins
✓ A digital twin refers to the digital representation of a real-world entity or system
✓ By 2020, Gartner estimates there will be more than 20 billion connected sensors
✓ Endpoints and digital twins will exist for potentially billions of things
✓ Please see link for examples

Augmented Analytics
✓ Machine Learning (ML) will transform how analytics content is developed and consumed

Source: Gartner. See link to Gartner’s Top 10 Strategic Technology Trends for 2019. See Full report here.
Gartner Top 10 Strategic Technology Trends for 2019

Quantum Computing (QC)
- QC operates on the quantum state of subatomic particles that represent information
- Elements denoted as quantum bits (qubits)
- Need to increase understanding of QC and how it can apply to business problems

Smart Spaces
- A smart space is a physical or digital environment
- Humans and technology-enabled systems interact in increasingly open, connected, coordinated and intelligent ecosystems

Immersive Experience
- VR, AR, and MR are changing the way in which people perceive the digital world
- This combined shift leads to the future Immersive User Experience

Digital Ethics and Privacy
- Digital ethics and privacy is a growing concern for individuals, organizations and governments

Blockchain
- Blockchain is a type of distributed ledger
- Promises to reshape industries by enabling trust
- Potential to provide transparency and reduce friction across business ecosystems
- High potential to lower costs, reduce transaction settlement times and improve cash flow

Source: See Link to Gartner's Top 10 Strategic Technology Trends for 2019. See Full report here.
Gartner’s Top 10 IoT Technologies for 2017 & 2018

1. IoT Security
2. IoT Analytics
3. IoT Device (Thing) Management
4. Low-Power, Short-Range IoT Networks
5. Low-Power, Wide-Area Networks
6. IoT Processors
7. IoT Operating Systems
8. Event Stream Processing
9. IoT Platforms
10. IoT Standards and Ecosystems

Source: Gartner, 2016. See link
Fundamentals of IoT
Definition of IoT

• IoT consists of a growing body of sensors around the world which collects and transmits data

• IoT also refers to the rules and events being applied to that data to make adjustments to systems and organizations

• Once data is stored, for example in the Cloud, analytics can be employed to generate useful and actionable insights

• Sensors are a key technology required to support IoT

• Data from sensors can be aggregated easily from various sources to generate actionable insights

Source: See Rossman’s "The Amazon Way on IoT: 10 Principles for Every Leader from the World’s Leading Internet of Things Strategies" [7], Pages 1-12.
IoT Core Technologies

SENSORS
DATA STORAGE / CLOUD
CONNECTIVITY
ANALYTICS

Source: Internet of Things for Architects by Perry Lea, Pages 27-30. See [10]
Data or an event is captured
Significant processing may occur in a device
Devices house:
- OS
- Software
- Power Supply
- Sensors that capture data and events

Broad set of options for connecting a device to the cloud or other device(s) exist
Examples:
- RFID
- Bluetooth
- Wireless
- Ethernet
- Others

Provides an expandable environment to process and store data
Considerations:
- Geography
- Speed
- Real-time requirements
- Volume of data
- Variety of data

Normally exists within the cloud environment
Includes:
- Database requirements
- Event notification
- Messaging
- Data visualization
- Reporting tools

Higher end rules engines
Learning algorithms
Recognizes key optimizations and adjustments to be made to devices
Often done in cloud
Sometimes done in devices

Note Rossman’s separation of Analytics and Machine Learning

Source: See Rossman’s “The Amazon Way on IoT: 10 Principles for Every Leader from the World’s Leading Internet of Things Strategies” [8], Pages 4-12.
Examples of Sensors

- Color
- Dust
- Earthquake
- Float
- Level
- Force
- Gas Leaks
- Humidity
- Moisture
- Image
- Camera
- Motion
- Multi-Function
- Pressure
- Proximity/Occupancy
- Tilt
- Touch
- Water Leaks

**Note:** There is an extensive set of IP on sensors: Please see CalTech, UCI.

**Source:** Internet of Things for Architects by Perry Lea, Pages 41-81. See [10].
Society is faced with a torrent of data

Data includes:

- Structured data such as transaction records
- Unstructured data such as still images, video, audio, and sensor data

 Biggest new source of data is IOT

- Data produced by sensors but harvested via the Internet

Sensors range from:

- Radio Frequency Identification (RFID) tags retailers use to track merchandise
- Video cameras that capture the flow of traffic

Human beings generate about 3 \textbf{exabytes} of data daily

- (1 Exabyte is $10^{18}$)

By 2020, there will be a data universe of \textbf{40 zettabytes} (1 followed by 21 zeroes)

- 1 zettabyte holds approximately 250 billion 2-hour High Definition (HD) movies

Source: John E. Kelly and Steve Hamm, See Reference [1], Pages 43-67.
Public, Private, and Hybrid Clouds

Left: Public Cloud, Middle: Private VS Public Cloud, Right: Hybrid Cloud

Source: Internet of Things for Architects by Perry Lea, Pages 347-348. See [10].
Five Cloud Services Models

Main criteria for distinction in models:

✓ Components that are privately managed
✓ Components that are cloud managed

Source: Internet of Things for Architects by Perry Lea, Pages 344-346. See [10].
Multi-tiered Anatomy of Cloud Architectures for IoT

1. A Cloud Service Provider sits outside the IoT edge device and presides over the wide area network.

2. Particular trait of IoT architecture is that **PAN** and **WAN** devices may not be IP-compliant.

3. Protocols such as **Bluetooth Low Energy (BLE)** and **ZigBee** are not IP-based.

4. Everything on the WAN including the Cloud is IP-based.

5. The role of the **Edge Gateway** is to perform the level of translation.

6. Another effect is the **Latency** and response time for events.

7. As you get closer to the sensor, you enter the realm of hard real-time requirements.

8. As we move up the stack, the gateway has the next best response time.

9. The Cloud component introduces another degree of latency over the WAN.

**Latency Effects of the Cloud.** Hard real time response is critical in many IoT applications and forces processing to move closer to the endpoint device.

*Source: Internet of Things for Architects by Perry Lea, Pages 356-359. See [10].*
Constraints of Cloud Architectures for IoT

Latency Effects of the Cloud. Hard real time response is critical in many IoT applications and forces processing to move closer to the endpoint device.

Source: Internet of Things for Architects by Perry Lea, Pages 356-359. See [10].
Three Sample Fog Topologies

Sample Fog Topology: Edge-fog device manages an array of sensors and may communicate in a M2M manner with another fog node.

Fog to Cloud Topology: Here a fog node establishes a link to a Cloud Provider.

Multiple Fog Nodes with a Single Master-Cloud

Source: Internet of Things for Architects by Perry Lea, Pages 370-376. See [10].
Multiple Fog Nodes with Multiple Cloud Providers. Clouds will be a Mixture of Public and Private Clouds.

Source: Internet of Things for Architects by Perry Lea, Pages 370-376. See [10].
Multi-Tier Fog Topology: Fog nodes stack in a Tier Hierarchy to Provide Additional Services or Abstraction

Rules engine, Mapping and Geolocation, Network Management

Image Recognition, Pattern Matching, GPU Assist, Monetary Archival

Edge Camera Aggregators, Feature Extraction, Denaturing

Lighting Manufacturer Control System

Source: Internet of Things for Architects by Perry Lea, Pages 370-376. See [10].
Non-IP Based Wireless Personal Area Networks (WPAN)
IP-Based WPAN and WLAN
Long-Range Communication Systems and Protocols
Non-IP Based WPAN

Non-IP Based Wireless Personal Area Networks (WPAN)
- Typically optimized for cost and energy usage
- Bridge sensors to a local net but not necessarily to the Internet or other systems
- First step in delivering IoT data from devices to the Internet

Examples of Non-IP Based WPANs

Bluetooth
- Low-power wireless connectivity technology used pervasively in technology from cell phones sensors, and keyboards to game systems
- Two modes of operation: Classic Bluetooth mode (BR/EDR) which is connection-oriented and Bluetooth Low Energy (BLE)
- Beaconing is a secondary effect of BLE and is important for IoT
  - Bluetooth is used to advertise on some periodic basis

ZigBee
- Proprietary and provides low-power wireless mesh networking

Z-Wave
- WPAN protocol used for consumer and home automation primarily

Source: Internet of Things for Architects by Perry Lea, Pages 111-177. See [10].
IP-Based WPAN and WLAN

- Protocol stacks for Bluetooth, ZigBee, and Z-Wave have similarities to a true TCP/IP protocol but do not inherently communicate over TCP/IP
- Adoptions of IP on ZigBee and IP over Bluetooth do exist

Internet Protocol (IP) Role in IoT
- Regardless of the protocol used at the sensor level, the sensor data will be ultimately be fed into a public, private or hybrid cloud for analysis, control or monitoring
- IP is the standard form of global communications for various reasons:
  - Ubiquity, Longevity, Standards-based
  - Scalability, Reliability, Manageability

Examples of IP-Based WPANs
- **6LoWPAN**
  - Brings IP addressability to the smallest and most resource-constrained devices
  - Principal advantage is that the simplest sensors can have IP addressability and act as a network citizen over 3G/4G/LTE/WI-FI/Ethernet routers
- **Thread**
  - Relatively new networking protocol for IoT and is based on IPV6
  - Principal target is home connectivity and home automation

Source: Internet of Things for Architects by Perry Lea, Pages 179-232. See [10].
Most prevalent form of communication is cellular radio and specifically cellular data.

4G-LTE is the modern standard for cellular communication and data:
- LTE is an abbreviation for Long-term Evolution technology
- Approved by the International Telecommunication Union (ITU)

LTE variety of Low Power Wide Area Networks (LPWAN) targeted for IoT:
- LTE Cat-0
- LTE Cat-1
- LTE Cat-M1 (eMTC)
- LTE Cat-NB

Proprietary LPWAN systems:
- LoRa
- SigFox
  - Similar to NB-IoT

Source: Internet of Things for Architects by Perry Lea, Pages 233-282. See [10].
A flood of information should be extremely valuable
Profusion of data is difficult to capture, make sense of, and move around
Less than 1% of digital data have been collected and actually analyzed
New generation of tools must be designed to handle the Four Vs of Big Data

1. **Volume**: Amount of data is increasing rapidly
2. **Variety**: Video, Geospatial, Web Pages, Speech
3. **Velocity**: May have to analyze data in motion
4. **Veracity**: Accuracy of data & conclusions are critical

Big Data is a digital expression of life in the raw

Source: John E. Kelly and Steve Hamm, See Reference [1], Pages 43-67
IoT business models will exploit the **information** collected by "things" in many ways

Examples of **information** that will be exploited:
- Understand customer behavior
- Deliver services
- Improve products
- Identify and intercept business moments

IoT demands **new analytic** approaches

New analytic tools and algorithms are needed

As data volumes increase through 2021, the needs of the IoT may **diverge** further from traditional analytics

Source: Gartner, 2016. See [link](#).
Analytics – Added Value

• The value of an IoT system is **not a single sensor event, or a million sensor event archived away**
  — A significant value of IoT is in the **interpretation** and **decision** made of that data
  — Value lies in what is **within** the data, what is **not in** the data, and what the **patterns** of data **tell us**

• **Three Phases of Analysis**

  1) **Data Ingest**
     - Data may need to be interpreted and analyzed in real-time as a streaming data flow
     - May also be archived and retrieved for deep analytics in the cloud
     - Data may need to be correlated with other sources in flight
     - Data may simply be logged and dumped to a data lake like a Hadoop database

  2) **Staging**
     - A messaging system like **Kafka** can route data to a stream processor, or batch processor, or both
     - Stream processing tolerates a continuous stream of data
     - In contrast, batch processing is efficient in dealing with high-volume data

  3) **Prediction and Response**
     - Information may be presented on some form of the dashboard
     - Information may be logged
     - System may respond to the edge device where corrective actions can be applied to correct some issue

Source: *Internet of Things for Architects* by Perry Lea, Pages 377-381. See [10].
# Basic Data Analytics in IoT

<table>
<thead>
<tr>
<th>Type of Analytics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preprocessing</strong></td>
<td>Filter out events of little interest, denaturing, feature extraction, segmentation, transform data to a more suitable form, adding tags.</td>
</tr>
<tr>
<td><strong>Alerting</strong></td>
<td>Inspect data; if it exceeds some boundary condition, then raise an alert. E.g. if temperature rises above a set limit in a sensor.</td>
</tr>
<tr>
<td><strong>Windowing</strong></td>
<td>A sliding window of events is created that only draws rules upon that window. Windows could be based on time (hour) or length (sensor samples).</td>
</tr>
<tr>
<td><strong>Joins</strong></td>
<td>Combine multiple data streams into a new single stream.</td>
</tr>
<tr>
<td><strong>Errors</strong></td>
<td>Millions of sensors will generate missing data, garbled data, and data that is out of sequence.</td>
</tr>
<tr>
<td><strong>Databases</strong></td>
<td>The analytics package will need to interact with some data warehouse.</td>
</tr>
<tr>
<td><strong>Temporal Events and Patterns</strong></td>
<td>Here, a sequence of events constitute a pattern of interest.</td>
</tr>
<tr>
<td><strong>Tracking</strong></td>
<td>Tracking involves when or where something exists, an event occurred, or when something doesn’t exist when it should exist.</td>
</tr>
<tr>
<td><strong>Trends</strong></td>
<td>Here, a rule is designed to detect an event based on time-correlated series data.</td>
</tr>
<tr>
<td><strong>Batch Queries</strong></td>
<td>Batch processing is typically more comprehensive and deeper than real-time stream processing.</td>
</tr>
<tr>
<td><strong>Deep Analytics Pathway</strong></td>
<td>In real-time processing, we make a decision on the fly that some event has occurred. Whether or not that event really should signal an alarm may require further processing that will not operate in real time.</td>
</tr>
<tr>
<td><strong>Models and Training</strong></td>
<td>The first-level model described in the deep analytics pathway may be an inference engine for a machine learning system.</td>
</tr>
<tr>
<td><strong>Signaling</strong></td>
<td>Action needs to be able to propagate back to the edge and sensor. The system needs to be bidirectional in communication.</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>Analysis tools need to be controlled – starting, stopping, reporting, logging, debugging facilities need to be in place.</td>
</tr>
</tbody>
</table>

Source: Internet of Things for Architects by Perry Lea, Pages 377-381. See [10].
Driving Forces for IoT Growth
Driving Forces for IoT

World Population Growth Rate

Connected Objects Growth Rate

Economics - Metcalfe’s Law
- McKinsey’s Report

Potential Impact of IoT
Billion IoT Connected Objects by 2020

Different Analyst and Industry Claims on the Number of Connected Things

Source: Internet of Things for Architects by Perry Lea, Page 14. See [10].
The disparity between human population growth versus connected thing growth. The trend has been a 20% growth of connected objects versus a nearly flat 0.9% percent human growth. Humans will no longer drive network and IT capacity.

Source: Internet of Things for Architects by Perry Lea, Page 15. See [10].
Demonstration of Metcalfe’s LAW (Value versus Cost)

\[ V \propto N^2 \]

Where:
- \( V \) = Value of Network
- \( N \) = Number of nodes within the network

**Metcalfe’s Law.** Value of a network is represented as proportional to \( N^2 \). The cost of each node is represented as \( kN \) where \( k \) is an arbitrary constant. In this case, \( k \) represents a constant of $10 per IoT edge sensor. The key takeaway is the crossover point occurs rapidly due to the expansion of value and indicates when this IoT deployment achieves a positive ROI.

Source: Internet of Things for Architects by Perry Lea, Page 31. See [10].
Tree of Potential IoT Impact

**Reducing Time to Market**
(Factory automation)

**Reducing Production Loss**
(Theft, spoilage of perishable)

**New Revenue Streams**
(Green energy solutions)

**Reducing Costs**
(In-home patient healthcare)

**Improving Supply Chain Logistics**
(Asset Tracking)

**Increasing Productivity**
(Machine learning Data analytics)

**Cannibalization**
(Nest replacing traditional thermostats)

**Saving of Lives**
(Improvement in information to First Responders)
Use Cases

- Industrial
- Consumer
- Retail
- Health
- Agriculture
- Transportation
- Energy
- Smart City
- Government
- Military
- Life Saving Things
Industrial IoT – IIoT Use Cases

✓ Preventive maintenance on new and pre-existing factory machinery
✓ Throughput increase through real-time demand
✓ Energy Savings
✓ Safety systems such as thermal sensing, pressure sensing, and gas leaks
✓ Factory floor expert systems

Source: Internet of Things for Architects by Perry Lea, Pages 16-25. See [10].
Consumer IoT Use Cases

- Smart Irrigation
- Smart garage doors
- Smart locks
- Smart lights
- Smart thermostats
- Smart security

Smart Home Gadgetry

- Health and movement trackers
- Smart clothing
- Smart wearables

Wearables

- Pet location systems
- Smart dog doors

Pets

Source: Internet of Things for Architects by Perry Lea, Pages 16-25. See [10].
Retail IoT Use Cases

01. **Targeted Advertising**, such as locating known or potential customers by proximity and providing sales information.

02. **Beaconing**, such as proximity sensing customers, traffic patterns, and inter-arrival times as marketing analytics.

03. **Asset Tracking**, such as inventory control, loss control, and supply chain optimizations.

04. **Cold Storage Monitoring**, such as analyzing cold storage of perishable inventory. Apply predictive analytics to food supply.

05. **Insurance Tracking of Assets**
   - **Insurance Risk Measurement of Drivers**
   - **Digital Signage Within Retail, Hospitality or Citywide**

*Source: Internet of Things for Architects by Perry Lea, Pages 16-25. See [10].*
Health IoT Use Cases

- In-home patient care
- Learning models of predictive and preventive healthcare
- Hospital equipment and supply asset tracking
- Pharmaceutical tracking and security
- Drug research
- Patient fall indicators
- Dementia and elderly care and tracking

Source: Internet of Things for Architects by Perry Lea, Pages 16-25. See [10].
Agriculture IoT Use Cases

- Smart irrigation and fertilization techniques to improve yield
- Smart lighting in nesting of poultry farming to improve yield
- Livestock health and asset tracking
- Preventive maintenance on remote farming equipment via manufacturer
- Drones-based land surveys
- Farm-to-market supply chain efficiencies with asset tracking
- Robotic farming
- Volcanic fault line monitoring for predictive disasters

Source: Internet of Things for Architects by Perry Lea, Pages 16-25. See [10].
Transportation & Energy IoT Use Cases

Transportation and Logistics IoT Use Cases
- Fleet tracking and location awareness
- Railcar identification and tracking
- Asset and package tracking within fleets
- Preventive maintenance of vehicles on the road

Energy IoT Use Cases
- Oil rig analysis of thousands of sensors and data points for efficiency gains
- Remote solar panel monitoring and maintenance
- Hazardous analysis of nuclear facilities
- Smart electric meters in a citywide deployment to monitor energy usage and demand
- Real-time blade adjustments as a function of weather on remote wind turbines

A trucking company might optimize fleet deployment based on Traffic dynamics or Truck telemetry.
Smart City Use Cases

- Pollution control and regulatory analysis through environmental sensing
- Efficiency gains and improved costs through waste management service on demand
- Energy efficiency of city lighting on demand
- Smart cameras to watch for crime and real-time automated AMBER Alerts
- Smart parking lots to automatically find best space parking on demand
- Bridge, street, and infrastructure wear and usage monitors to improve longevity and service
- Microclimate weather predictions using citywide sensor networks
- Improved traffic flow and fuel economy through smart traffic light control and patterning
- Smart snow ploughing based on real-time road demand, weather conditions, and nearby ploughs
- Smart irrigation of parks and public spaces, depending on weather and current usage

Source: Internet of Things for Architects by Perry Lea, Pages 16-25. See [10].
Government & Military IoT Use Cases

- Terror threat analysis through IoT device pattern analysis and beacons
- Swarm sensors through drones
- Sensor bombs deployed on the battlefield to form sensor networks to monitor threats
- Government asset tracking systems
- Real-time military personal tracking and location services
- Synthetic sensors to monitor hostile environments
- Water level monitoring to measure dam and flood containment

Source: Internet of Things for Architects by Perry Lea, Pages 16-25. See [10].
Internet of Life Saving Things – IoLST Use Cases

- Internet of Life-Saving Things
  - Also known as Public Safety Things
  - Collection of connected devices and sensors
  - Used by First Responders to keep themselves safe
  - Also used to protect the lives of people and the safety of property!
  - Many IoT Devices also have a public safety purpose!

Texas City Refinery Fire, March 23, 2005
West, Texas Fertilizer Explosion, April 17, 2013

I5 – Amtrak Derailment, December 18, 2017

References: Keynote Address by Bill Schrier, Seattle Times, Image by CNN, Image by ABC News
THE PROBLEM
Initiative to Extend Product Lines by Leveraging IoT

THE SOLUTION
Prove Concepts Incrementally Through Prototyping

GENERAL APPROACH
The Incremental Commitment
SPIRAL MODEL

Case Study
There is a company initiative to explore how IoT can be adopted to create new products or extend existing product lines.

Cognizant of core technology stack for IoT:
- Sensors
- Connectivity
- Cloud/Data
- Analytics

However, there are no real requirements:
- Really a research project in Emerging Technology

Decided to collaborate and brainstorm a product idea.

Broad product requirements:
- Develop an IoT Device that collects information that First Responders could find valuable in their mission to save lives
- Show progress incrementally to stakeholders:
  - VP of Engineering
  - Director of Engineering
  - Engineering Community
Challenge: Prove End-to-End Pathway

Device Requirements
- Support multiple sensors
- Support wireless connectivity
- Small form factor

Key Connectivity Requirements
- Support wireless connectivity
- Work even when there is no wireless connection

IOT = f (Sensors, Connectivity, Cloud, Analytics)

Connectivity
- AT&T LTE Network
- AT&T LTE-M Network
- T-Mobile Network
- Verizon Network
- FirstNet Network
- Satellite

Cloud/Data
- Amazon Web Services
- Microsoft Azure
- IBM Cloud
- Salesforce
- AT&T Cloud

Analytics
Development Approach

- General Approach (Barry Boehm, Jo Anne Lane, Supannika Koolmanojwong, and Richard Turner. See Reference [9])
  - Incremental development with stakeholders’ commitment
  - Get evidence to fortify concepts
  - Prototyping to reduce risks
  - Always be open to discard/exit if not feasible!

- Why prototyping?
  - It will help us identify and reduce risks before we make a huge commitment
  - This will make it possible to involve our stakeholders at each critical phase
  - It will help us determine if development should continue

- Question we need to ask: Should we take the off-ramp now?

Source: The Incremental Commitment SPIRAL MODEL by Barry Boehm, Jo Anne Lane, Supannika Koolmanojwong, and Richard Turner. See [9].
Prototyping Plan

- Get familiar with IoT kits
- Select one or more kits for evaluation

- Using the selected IoT kits, demonstrate the capability to:
  I. Capture data using built-in sensors
  II. Transfer that data to the cloud using a wireless LTE network such as AT&T’s LTE network

- High Priority Use Cases
  I. Send data to an IoT platform such as AT&T’s M2X
  II. Display the data sent to the cloud and prove that the data is accurate

- Lower Priority Use Cases
  I. Send data to a service running in Amazon Web Services
  II. Send data to a service running in Microsoft Azure
  III. Send data to services running in other clouds such as IBM or Salesforce

- Each use case will be developed incrementally using prototyping
Critical Review

Criteria for Evaluation
1. Quality?
2. Performance?
3. Scalability?
4. Adaptability to embedded?
5. Useful in product?
6. Worth additional investment?
Overview of IoT Kit

Display Dashboard for Edge Device

Source: AT&T IoT Starter Kit [2nd Gen] Quick Start Guide
Overview of IoT Kit

- WiFi Module
- User LEDs
- USB-OTG
- STLink USB
- Sub-GHz
- Arduino Connectors
- Bluetooth Low Energy
- MEMS Microphones
- Temperature and Humidity Sensor
- Pressure Sensor
- Magnetometer
- Gyroscope & Accelerometer
- Time of Flight Sensor
- STM32L475VG MCU
- NFC
- Reset Button
- User Button

Source: AT&T IoT Starter Kit (STM32 LTE-M) Quick Guide
Demo #2 - AT&T IoT Starter Kit (STM32 LTE-M)

Flow from Sensors to Cloud

Source: AT&T IoT Starter Kit (STM32 LTE-M) Quick Guide
Thoughts On IoT Security
IoT Security Considerations

- The IoT introduces a wide range of new security risks and challenges to:
  - The IoT devices themselves
  - Their platforms and operating systems
  - Their communications
  - Systems to which they are connected

- Three forms of prevalent IoT security attacks
  1. **Mirai**: Most damaging denial of service attack in history that spawned from insecure IoT devices in remote areas
  2. **Stuxnet**: A nation-state cyber weapon targeting industrial SCADA IoT devices controlling substantial and irreversible damage to Iran’s nuclear program
  3. **Chain Reaction**: A research method to exploit PAN area networks using nothing but a lightbulb-no internet needed

Source: Mckinsey Global Institute, "The Internet of Things: Mapping the value beyond the hype", 06/2015.

Source: Gartner, 2016. See link.
IoT Security Considerations

- Security technologies **will be required to**:
  - Protect IoT devices and platforms from both information attacks and physical tampering
  - Encrypt their communications
  - Address new challenges such as:
    - Amplification Attack
    - Botnets
    - Slide Channel Attack
    - Distributed Denial of Service (DDoS)
    - Man-in-the-Middle Attack (MITM)

Source: Gartner, 2016. See [link].
Source: McKinsey Global Institute, "The Internet of Things: Mapping the value beyond the hype", 06/2015.
Source: Internet of Things for Architects by Perry Lea, Pages 427-473. See [10].
IoT Security Considerations

- IoT security will be complicated because:
  - Many "things" use simple processors and operating systems
  - These processors and operating systems may not support sophisticated security approaches

- Experienced IoT security specialists are scarce

- Security solutions are currently fragmented and involve multiple vendors

- New threats will emerge through 2021 as hackers find new ways to attack IoT devices and protocols

- Long-lived "things" may need:
  - Updatable hardware and
  - Software to adapt during their life span

Source: Gartner, 2016. See link.  
Source: Mckinsey Global Institute, "The Internet of Things: Mapping the value beyond the hype", 06/2015.  
Source: Internet of Things for Architects by Perry Lea, Pages 427-473. See [10].
## Essential IoT Security Terms

### Attack and Threat Terms

<table>
<thead>
<tr>
<th>Amplification Attack</th>
<th>Replay Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Spoof</td>
<td>RCE Exploit</td>
</tr>
<tr>
<td>Banner Scans</td>
<td>ROP Attack</td>
</tr>
<tr>
<td>Botnets</td>
<td>Return-to-libc</td>
</tr>
<tr>
<td>Brute Force</td>
<td>Rootkit</td>
</tr>
<tr>
<td>Buffer Overflow</td>
<td>Slide Channel Attack</td>
</tr>
<tr>
<td>C2</td>
<td>Spoofing</td>
</tr>
<tr>
<td>Correlation Power Analysis Attack</td>
<td>SYN Flood</td>
</tr>
<tr>
<td>Dictionary Attack</td>
<td>Zero-Day Exploits</td>
</tr>
<tr>
<td>Distributed Denial of Service (DDoS)</td>
<td></td>
</tr>
<tr>
<td>Fuzzing</td>
<td></td>
</tr>
<tr>
<td>Man-in-the-Middle Attack (MITM)</td>
<td></td>
</tr>
<tr>
<td>NOP sleds</td>
<td></td>
</tr>
</tbody>
</table>

### Defense Terms

<table>
<thead>
<tr>
<th>Address Space Layout Randomization</th>
<th>Private Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black Hole (Sinkhole)</td>
<td>Root of Trust (ROT)</td>
</tr>
<tr>
<td>Data Execution Prevention (DEP)</td>
<td>Secure Boot</td>
</tr>
<tr>
<td>Deep Packet Inspection (DPI)</td>
<td>Stack Canaries</td>
</tr>
<tr>
<td>Firewall</td>
<td>Trusted Execution Environment</td>
</tr>
<tr>
<td>Guard Bands and Non-Executable Memory</td>
<td></td>
</tr>
<tr>
<td>Honeypots</td>
<td></td>
</tr>
<tr>
<td>Instruction-Based Memory Access Control</td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection System (IDS)</td>
<td></td>
</tr>
<tr>
<td>Intrusion Prevention System</td>
<td></td>
</tr>
<tr>
<td>Milkers</td>
<td></td>
</tr>
<tr>
<td>Port Scanning</td>
<td></td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td></td>
</tr>
</tbody>
</table>

**Source:** Internet of Things for Architects by Perry Lea, Pages 427-473. See [10].


Source: Internet of Things for Architects by Perry Lea, Pages 427-473. See [10].
Thank You!


8. Bob Karschnia, “Industrial Internet of Things (IIoT) benefits, examples”, Control Engineering, 06/03/2015. See link


