IoT and Smart Infrastructure
Standardisation Perspective

Aurindam Bhattacharya
Centre for Development of Telematics

www.cdot.in
The Internet of Things (IoT) is the network of physical objects/devices, vehicles, buildings and other items—embedded with electronics, software, sensors with a network connectivity that enables these objects to collect and exchange data.

British entrepreneur Kevin Ashton first coined the term in 1999 while working at Auto-ID Labs (originally called Auto-ID centers, referring to a global network of objects connected to radio-frequency identification, or RFID)

According to Gartner, The Internet of Things (IoT), would have an installed base that will grow to 26 billion units by 2020.

ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of Things by 2020.
Technology roadmap: The Internet of Things

- **Cost reduction leading to diffusion into 2nd wave of applications**
  - Demand for expedited logistics
    - RFID tags for facilitating routing, inventorying, and loss prevention
- **Supply-Chain Helpers**
- **Vertical-Market Applications**
  - Surveillance, security, healthcare, transport, food safety, document management
  - Locating people and everyday objects
- **Ubiquitous Positioning**
  - Teleoperation and telepresence: Ability to monitor and control distant objects
  - Miniaturisation, power-efficient electronics, and available spectrum
  - Software agents and advanced sensor fusion
- **Physical-World Web**
So What does Smart Infrastructure Mean to us

- Electric toothbrush: Automatically reorders brush heads and shares brushing habits with your dentist.
- Automobile: Maps traffic in real time; allows others to track your location.
- Computer: Offers centralized control for remote interfacing to any other device.
- Media player: Remotely orders new songs and videos.
- Alarm clock: Has remote programs and custom tones; turns on coffeemaker.
- Refrigerator: RFID tags reorder groceries as needed and suggest recipes.
- VoIP phone: Provides automatic updates, integration, and forwarding.
- Printer: Automatically reorders toner and paper as needed.
- Microwave: Automatically sets cook cycle with RFID recognition.
- Coffeemaker: Has custom settings for each coffee type; starts when alarm goes off.
- Oven: Allows settings to be changed from a computer or phone.
- HVAC: Controls temperature and lights for maximum efficiency.
- Television: Enables immediate ordering of products seen on commercials.
- Smart scale: Measures and sends weight info for progress tracking.
- Cell phone: Securely performs identification and verification for payments.
- Vending machine: Automatically reorders supplies before it’s empty.
- Exercise equipment: Recognizes individual users and tracks workout schedules.
More Devices than people

- Smart phones
- Smart Tablets
- Smart desktops and Laptops
- Data-enabled phones
- Smart Consumer appliances
- Embedded systems
- Sensors
- RFID
Potential Smart Infrastructure services

Everything Else you can think of

1. Vending Machines
   Vending Machines are connected to a centralized server

2. ATM / POS
   ATM / POS connected to the bank's network

3. Fleet Tracking
   The vehicles can be traced through the path they follow

4. Emergency Call / Navigation
   In the case of an emergency, a signal is sent through mobile connection

5. Public Transport
   Buses are monitored in real-time

6. Industrial Telemetry
   Sensors are monitored in real-time

7. Smart Metering for Electricity
   The electricity smartgrids reports a measurement every certain period

8. Smart Metering for Water
   The water smartgrids reports a measurement every certain period

9. Smart Metering for Gas
   The gas smartgrids reports a measurement every certain period

10. Machine-to-Machine

01-12-2016 C-DOT Confidential
View Of 2020 and Beyond: EVERYTHING connected

Drivers
- Entertainment, security, healthcare,
- Productivity, new revenue streams
- Sustainability and regulation

Devices connecting the masses, such as Consumer Electronics and Home Automation

Specialized IoT/M2M applications across all government, industry & society

Drivers
- Ubiquity of Broadband
- Declining cost of connectivity
- Propagation of embedded IoT/M2M Devices

Enablers
Technology Trends

- **Field Domain**
  - Sensor Technologies –Long (endless!) battery life, Self healing, Secure, Adaptive
  - Wireless Technologies like Sensor Networks, Wi-Fi, Zigbee, 6 LowPAN, LoRa etc.

- **Infrastructure Domain**
  - Evolving (It has to change significantly in order to cater to the needs of the huge explosion of IoT)

- **Head End**
  - Cloud, Big Data, New Age Analytics
Trends envisaged for IoT/M2M Technologies

- Towards 2020, technological development will be shaped by the force-multiplying effects of:
  - The convergence of nanotechnology, biotechnology, materials technology, and information and communications technology.
  - The acceleration of technological development.
  - Growing information exchange between developed and developing countries.
  - Developing countries participating in technology development

Towards 2020 we expect to see major progress in intelligent technology, such as
  - Nearfield communication (NFC) sensors,
  - smart surveillance and security applications and
  - Smart robots,

which will enable automation of more activities. Technology will take over more domains and functions as robot technology improves in quality and stability and prices for advanced technologies decline and labour costs increase.
The development of the Internet of Things and ambient intelligence will allow managers to develop a much better understanding of how people are using buildings, cars, wearable devices etc. leading to new maintenance approaches, better designs, and more productive and cost effective technologies.

This development will also lead to a number of ethical and security challenges, for which industry should develop contingency plans.

For example:

i. Which data are you permitted to store, and for how long?

ii. Who owns the data collected from individuals?

iii. Who is responsible for securing and protecting these data?
Stakeholders of IoT/M2M
All are hidden behind the wall and the users are without any choice.
A lot of traffic (upload) gets generated in proprietary manner from the sensors to the respective Servers running the business process. Here the TSPs/ISPs networks are used as mere transport.

**No interoperability...No Common Service Function**
The registration, discovery, security etc are taken care of by the respective Business Functions themselves.
Present Landscape of Non-standardised M2M/IoT Deployment

Now imagine the data being shared between multiple business processes

And there are billions of these devices...!!

Gateway
PAN
Devices/Sensors

Gateway
PAN
Devices/Sensors

Gateway
PAN
Devices/Sensors

Gateway
PAN
Devices/Sensors
Need For Standardisation

• So far the IoT/M2M industry is vertical Centric and the Telecom Network is merely used as a transport. However, these networks may need to be optimised to cater for these new solutions which have very different behaviour from what is currently prevailing.

• Standardization is required in order to deliver cost-effective IoT/M2M solutions, and allow this market to take off.

• Many component-level standards already exist, addressing various radio interfaces, different meshed or routed networking choices, or offering a choice of identity schemes. Each is optimised for a particular application scenario and there is therefore a degree of fragmentation.

• Now, efforts are being made by SDOs like OneM2M to bring all these pieces together, and identify the standardization gaps which exist.
## Standardization approach

<table>
<thead>
<tr>
<th>Use cases</th>
<th>Requirements</th>
<th>Architecture APIs and protocols</th>
<th>Test and Interop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automotive</td>
<td>Security &amp; privacy</td>
<td>IP communications</td>
<td>Reference points</td>
</tr>
<tr>
<td>Home</td>
<td>Device Management</td>
<td>Restful webservices APIs</td>
<td>Device certification</td>
</tr>
<tr>
<td>Energy</td>
<td>Data exchange</td>
<td>Reuse of existing protocols</td>
<td>Open source</td>
</tr>
<tr>
<td>E-Health</td>
<td>Interworking</td>
<td>Semantics framework (future)</td>
<td></td>
</tr>
</tbody>
</table>

- **Automotive**: Security & privacy
- **Home**: Device Management
- **Energy**: Data exchange
- **E-Health**: Interworking
- **Reference points**: Device certification
- **Open source**: Semantics framework (future)
**Landscape of IoT/M2M Architecture**

**Pipe (vertical):**
1 Application, 1 NW,
1 (or few) type of Device

**Horizontal (based on common Layer):**
Applications share common infrastructure, environments, network elements & data

- **Business Application #1**
- **Business Application #2**
- **Business Application #n**

**Common Service Layer**

- **Transport Network 1**
- **Transport Network 2**

**Device**

**Gateway**

**Local N/W**

**Business platform**

**Application Entity**

**Common Service Entity**

01-12-2016

C-DOT Confidential
Standard End to End IoT/M2M Solution

- Standardized APIs for Diverse Devices
- Standard APIs, Access, Security & Device Management Features
- Cellular Core Network
- IP Network
- Standardized APIs to Diverse Verticals

**M2M Devices**
Cellular, WLAN, WPAN (Zigbee, 6LoWPAN, Bluetooth), Wireline

**M2M Gateway**
Enables cellular & non-cellular M2M devices to communicate through operator networks. Provides localized Service Capabilities to offload network

**M2M Server**
Service Provider’s M2M Service Platform, offering Service Capabilities to Diverse M2M Verticals (Device/Data Access, Device Management, Security, Billing, Service Discovery, etc.)
Standard Based Architecture approach

Currently developed solutions are similar and vertically integrated, with limited integration of data models (Zigbee, DLMS for smart meters, etc.).

Horizontal framework, Restful API
Objects represented as resource
Access control policy to access resource

IoT will be based on ontologies (formal description of concepts and relationships, e.g. W3C Semantic Sensor Network) as well as big data frameworks

TOMORROW
IoT ready
IoT enabled
What is oneM2M?

- A global partnership among Standards Defining Organizations (SDOs) and Industry Associations like:
  - ARIB (Association of Radio Industries and Businesses, Japan), ATIS (Advancing Transformation of the ICT Industry, America), CCSA (China Communications Standards Association, China), ETSI (European Telecommunications Standards Institute, Europe), TIA (Telecommunication Industries Association, America), TSDSI (Telecommunications Standards Development Society, India), TTA (Telecommunications Technology Association, Korea), and TTC (Telecommunications Technology Committee, Japan).
  - Additional partners contributing to the oneM2M work include: the BBF (Broadband Forum), Continua, GlobalPlatform, HGI (Home Gateway Initiative), the New Generation M2M Consortium - Japan, and OMA (Open Mobile Alliance).
  - [C-DOT is also partner Type I (through TSDSI) contributing to the standards]

- In simple terms the main goal to develop technical specifications for an IoT/M2M Service Layer
  - A software platform to make IoT/M2M devices/applications communicate with each other in a secure and efficient manner
“ANY APP”

“ANY NETWORK”

“ANY DEVICE”

application creation & analytics

connectivity, onboarding, AAA, management, security, ...

devices & gateways

sensors
Layered model for high-level architecture of oneM2M

- **CSE (Common Service Entity):**
  - Offer common functionalities exposed through the Reference Points.
  - CSE contains Common Service Function Modules (CSF).
  - CSE and CSF are represented by Restful resource management and message flows.

```
Application Entity (AE)
→ Mca Reference Point

Common Services Entity (CSE)
→ Mcc Reference Point

Underlying Network Service Entity (NSE)
→ Mcn Reference Point
```
## Architecture

<table>
<thead>
<tr>
<th>Reference Point</th>
<th>One or more interfaces - Mca, Mcn, Mcc and Mcc’ (between 2 service providers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Services Entity</td>
<td>Provides the set of &quot;service functions&quot; that are common to the IoT/M2M environments</td>
</tr>
<tr>
<td>Application Entity</td>
<td>Provides application logic for the end-to-end IoT/M2M solutions</td>
</tr>
<tr>
<td>Network Services Entity</td>
<td>Provides services to the CSEs besides the pure data transport</td>
</tr>
<tr>
<td>Node</td>
<td>Logical equivalent of a physical (or possibly virtualized, especially on the server side) device</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Layer</th>
<th>AE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Layer</td>
<td>CSE</td>
</tr>
<tr>
<td>Network Layer</td>
<td>NSE</td>
</tr>
</tbody>
</table>

- Application Service Node
- Middle Node
- Infrastructure Node

01-12-2016

C-DOT Confidential
Typical IoT/M2M use case in Power Sector using C-DOT IoT/M2M Solutions
C-DOT’s IoT/M2M Offering

• A Standard based IoT/M2M Platform
  • Middle Node (Gateway in the Device Domain)
  • Infrastructure Node (in Infrastructure Domain)

Having the Common Service Entity (Common Service Layer) providing the Common Service Functions described above.

It would enable the industry to develop Standard based Applications which would reduce the development, test and deployment lifecycles.
Advantages of C-DOT IoT/M2M Platform

**Combat fragmentation**
- Healthy eco-system with economies of scale
- More partnering choices and opportunities for M2M/IOT industry stakeholders

**Lower CAPEX**
- Standardized protocols / APIs -> simplifies application development/deployment
- Cross-vertical standards -> same devices and back-ends in different industries

**Lower OPEX**
- Standard features to use networks more efficiently -> get better tariffs
- Flexibility for verticals -> utilize best transport network meeting business needs

**Time to Market**
- Reduced development, test and deployment lifecycles through focusing on core business (application logic)
Typical Standards’ Compliant Smart City Architecture

- Economic development
- Sustainability
- Higher quality of life

- Citizen and stakeholder engagement
- Predictability
- Cost avoidance
- New products and services
- Competitive advantage

- Open data and transparency
- Manage risk
- Increase productivity
- Better citizen service
- Innovation

- Big data and analytics
- Mobility
- Social
- Cloud

Cloud

Standards compliant IoT/M2M Application

Proprietary Application

Infrastructure Node

IoT/M2M Gateways

Core Network

- LTE
- 2G
- 3G
- IN
- ADN
- MN
- PAN
- ASN
- MAN
- Optical

Actuators

Sensors

Surveillance Cameras

SERVICES

01-12-2016 C-DOT Confidential
Thank You