In the framework of SESEI

In association with CII Confederation of Indian Industry

3rd Indo-European Conference on Standards and Emerging Technology

26th April, 2018 – New Delhi

INFORMATION & COMMUNICATION TECHNOLOGY (ICT)

COVERING M2M/IOT AND ITS ROLE IN SMART CITY + CYBER SECURITY

Prepared by Confederation of Indian Industry

Presented by N. Kishor Narang

INFORMATION COMMUNICATION TECHNOLOGY (ICT)

COVERING M2M/IoT and Its ROLE IN SMART CITY + CYBER SECURITY

- M2M/IoT Eco-System, Market Dynamics & Potential
- Policy Initiatives & Standardization
- Gaps & Challenges
- Conclusions and Recommendation

Today's Challenge: Digitization - Data Deluge

By 2020, 3.4 million Things shall be added to Internet every Minute

M2M/IOT ECO-SYSTEM

Market Dynamics & Potential

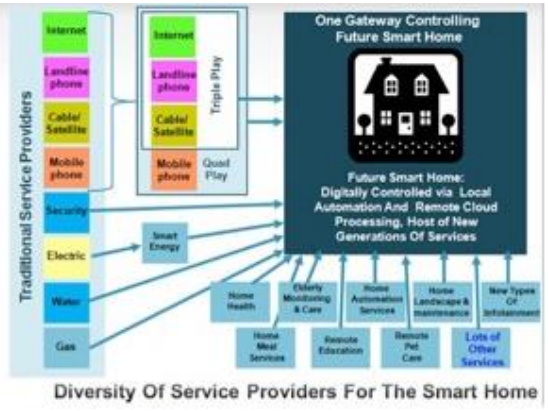
M2M/IoT Eco-System, Market Dynamics & Potential

- Connectivity & M2M/IoT
- M2M/IoT & Roll Out of 5G Networks
- Common Service Layer
- Application Protocols and Messaging Middleware
- Cloud, Big Data & Analytics
- M2M/IoT Networks – Security
- M2M/IoT in Smart Cities & Smart Infrastructure
- M2M/IoT Industry Growth in India - Key Drivers
- Adoption of M2M/IoT in India
- Communication and Network Infrastructure
- M2M/IoT - Technology Innovations
- M2M/IoT – Readiness of Major Indian Operators

M2M… to … IoT - Defining the IoT Systems:

- IoT is about “Connected Intelligence”, a sort of “universal global neural network” in the cloud..

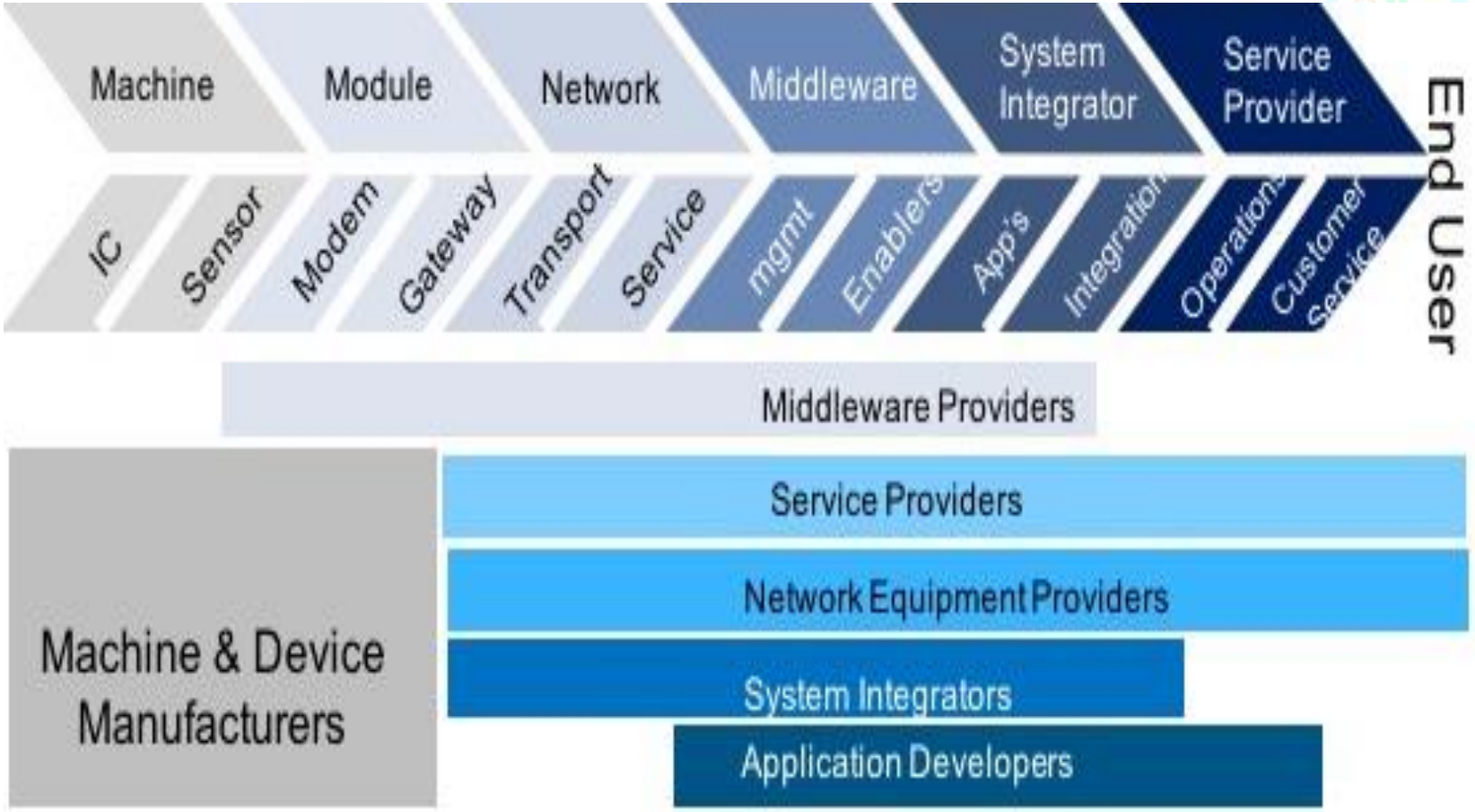
- It is believed that the Internet of Things, or the ability for consumer devices and appliances to communicate with one another via Web access and a complex system of embedded sensors, will ***"enable a wide range of new applications and services while raising many new challenges"***.



Diversity Of Service Providers For The Smart Home

Internet of Things is all about “heterogeneous” and “aware” devices interacting to simplify people’s life in some way or the other.

M2M/IoT Value chain:



In this absolutely heterogeneous scenario, coming up with common harmonized standards is a major hurdle.

7 Layers of Information Flow in IoT Paradigm

NATURE of ANALYSIS

COGNITIVE
Learn dynamically ?

PRESCRIPTIVE
What are the best outcomes ?

PREDICTIVE
What could happen ?

DESCRIPTIVE
What has happened ?

DISCOVERY
What do we have ?

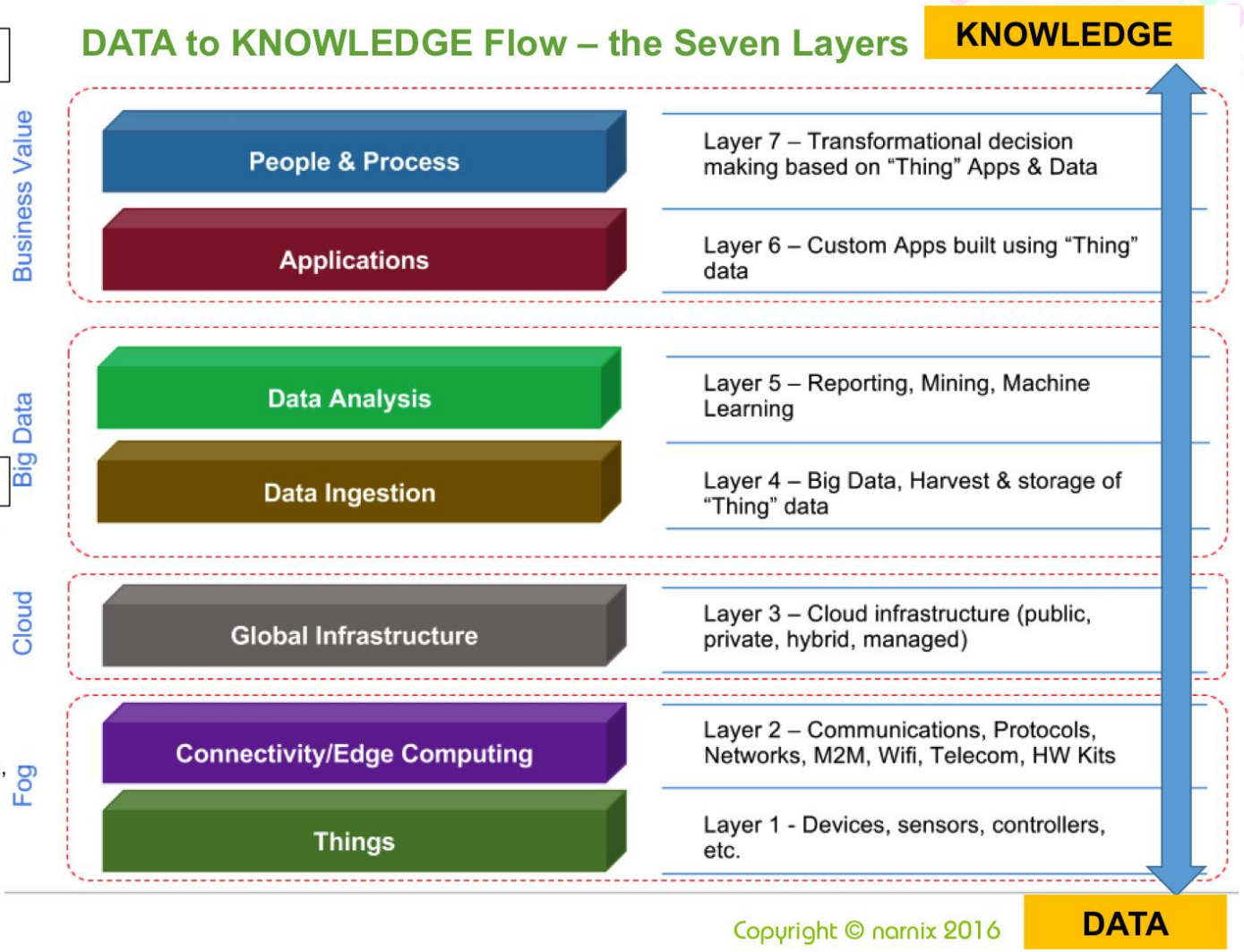
NATURE of INGESTED DATA

DATA @ REST (VOLUME)
Archival/Static data (TBs) in Data stores

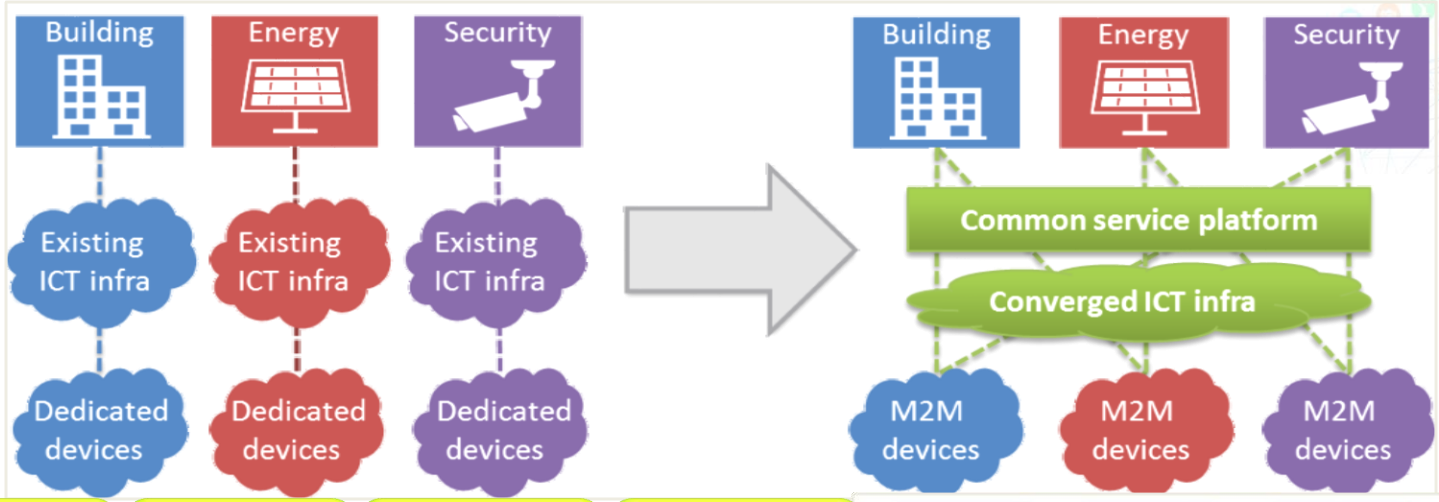
DATA @ MOTION (VELOCITY)
Streaming data

DATA @ MANY FORMS (VARIETY)
Structured/Unstructured, Text, Multimedia, Audio, Video

DATA @ DOUBT (VERACITY)
Data with uncertainty that may be due to incompleteness, missing points, etc.,



Common Service Layer: Framework for Interoperability



Delivering homogeneity in heterogeneous paradigm

The Security aspect of the IoT..

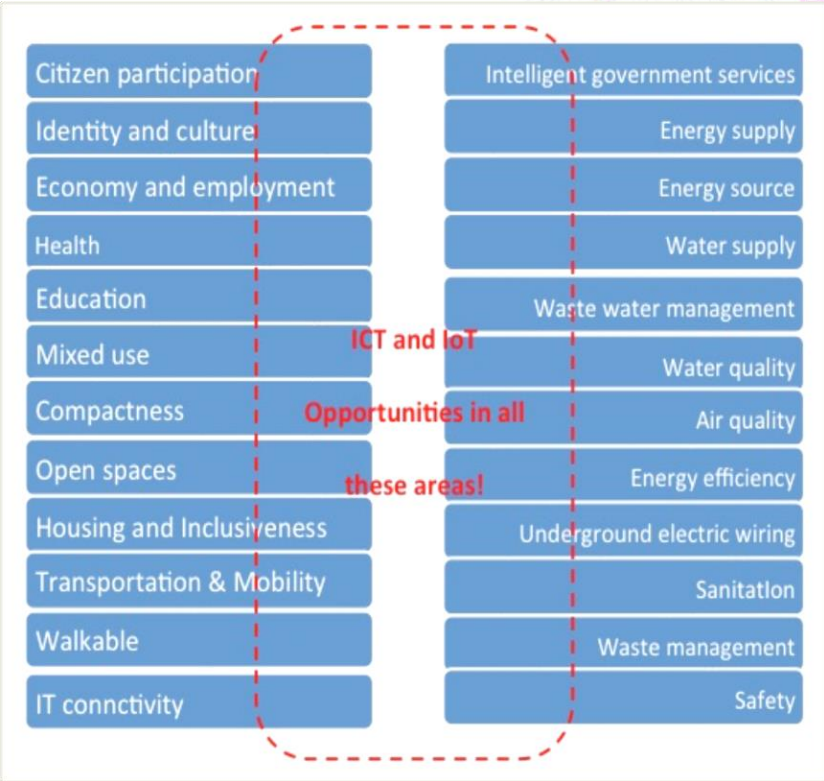
- The importance of security for IoT infrastructure and platforms cannot be overemphasized. Rather than specific products or services, the next important developments in IoT should be overarching standards, policies, security frameworks and infrastructures.
- IoT is dependent on a wealth of data being collected from numerous devices connected across different interfaces and locations within the Enterprise, while carrying sensitive company or customer information.
- Any kind of security breach could compromise the organization's customers, workers or even the business itself.

A stable secure technology platform with proven security standards will be imperative for IoT proliferation. This isn't only about the protection of individuals and their privacy but about safeguarding any nation's digital ecosystem and the economy therein.

Smart Cities & Smart Infrastructure

A sample Indian business case for next 5-10 years:

- 250 million Smart Electricity Meters are going to be procured & deployed under the NSGM (National Smart Grid Mission).
- All these **Smart Meters** are going to use **250 million Communication Modules** and minimum **0.5 million Gateways/DCUs** (Data Concentrator Units).
- **Smart Streetlights** are going to use more than **100 million Communication Modules** and at least **half a million of DCUs/Gateways**…
- **Smart Buildings** are going to deploy more than **50 million smart Sensors** and at **least 100K – 200K DCUs/gateways…**
- **Automobile**s shall be using at least **100-200 million** communication nodes for Vehicle O & M, V to V, V to I & other telematics applications…
- Similarly, various applications of the Smart Infrastructure paradigm like Smart Water, Smart Gas, Smart Traffic, Smart Environment, Smart sewage Disposal etc. are going to use a few billions of Smart Sensors with Communication Modules



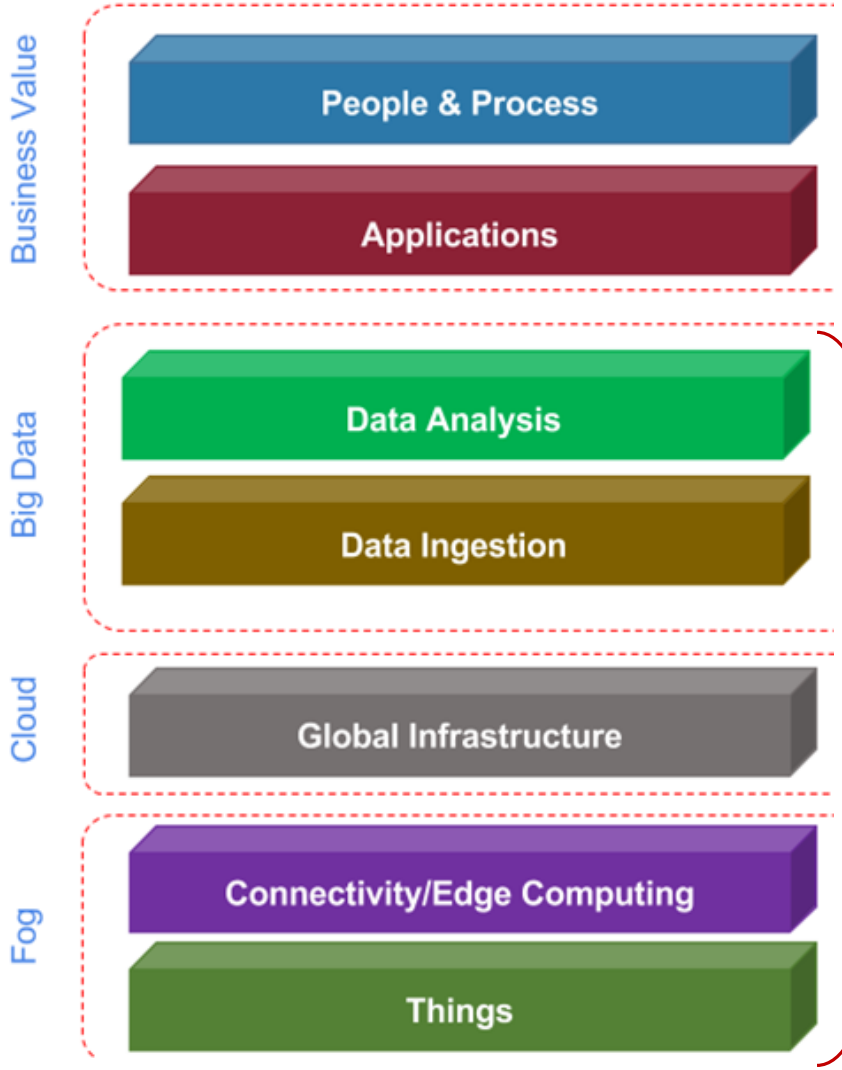
To summarize, India ALONE, is going to need a minimum of **5 - 10 billion Communication modules** to be integrated into the Smart Sensors and Controllers and **10– 50 million Gateways** that shall be needed to operate and maintain the ***Nation Wide Critical Infrastructure*** that needs to be deployed to enable and empower the citizens to lead a sustainable, safe and secure life …

POLICY INITIATIVES & STANDARDIZATION

Policy Initiatives & Standardization

- Government Policies on M2M/IoT- Centre and States
  - National Telecom Policy
  - National Telecom M2M Roadmap
  - IoT Policy – Centre and States
- M2M/IoT standardization
  - Convergence of Vertical and Horizontal Standardization
  - European Telecommunications Standards Institute (ETSI)
- Current Policy & Standardization Activities in India
  - BIS LITD 27
  - BIS LITD 28
  - TSDSI
  - MoC/TEC & MoC/WPC
  - TRAI
  - MeitY
  - Testing and Certification

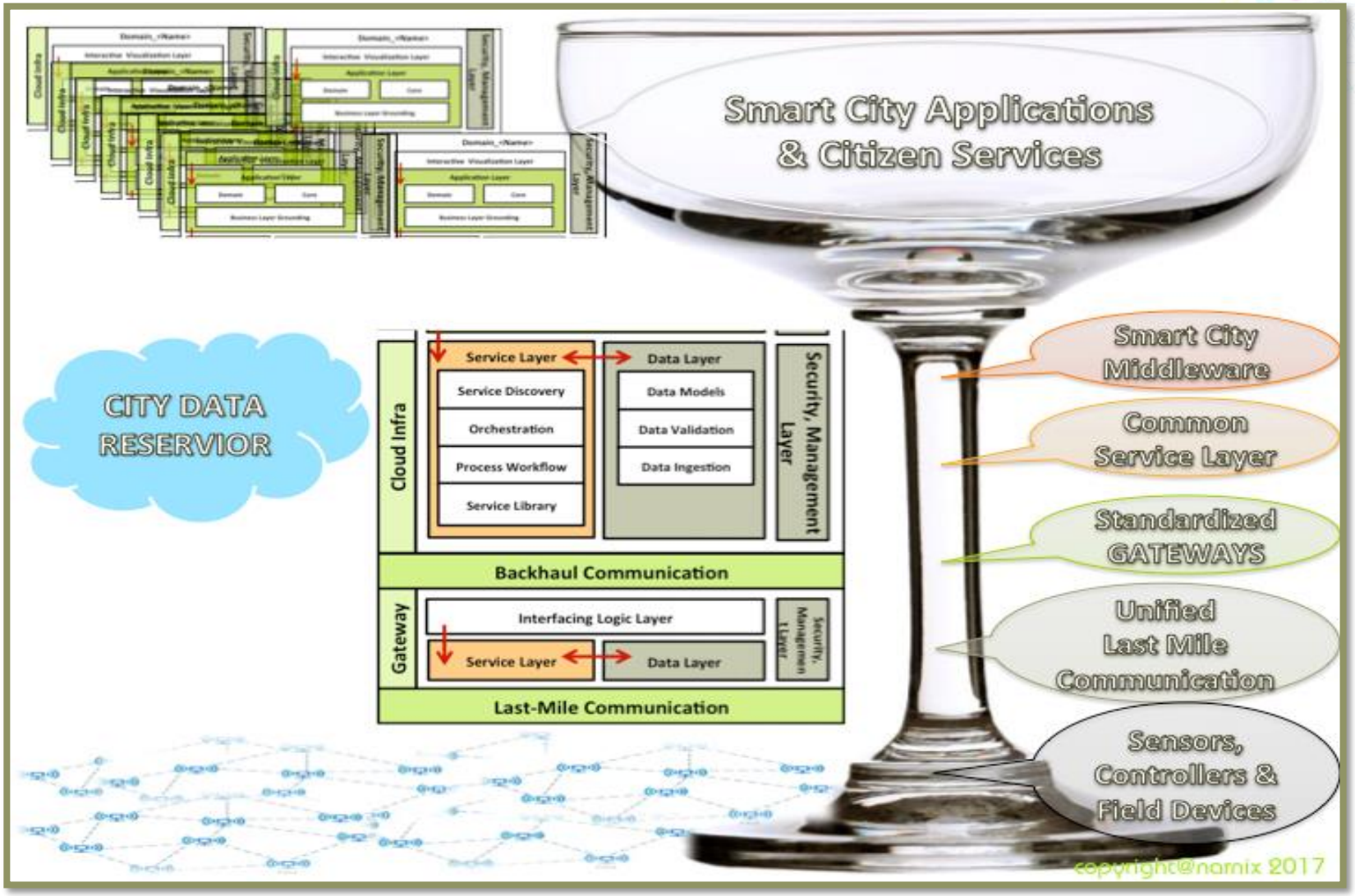
Mapping the IoT Paradigm to Smart City Infrastructure



Physical Infrastructure	Social Infrastructure	Economic Infrastructure	Institutional Infrastructure

The application needs **change** (as part of the users' requirement) to derive value from different infrastructure pillars, **but** the ICT and IoT **backbone remains (or should remain) the SAME !!!**

Classic Saucer Champagne Glass Architecture



GAPS & CHALLENGES

Gaps & Challenges

- Problem Statement
- IoT Paradigm & Challenges
- Challenges in fast growth of IoT
  - Service provider challenges
- The Security aspect of the IoT
- Current Challenges Smart Cities including Smart Infrastructure
  - Other important Smart City issues
- Standardization Imperatives

IoT Paradigm & Challenges

It is difficult for innovation to happen across disjointed platforms & technologies

The IoT paradigm is expected to be a solution for all the problems and expected to have the characteristics of a Homogeneous Network of Heterogeneous Devices… it is expected to address applications in multiple diverse domains like Industrial, Consumer, Infrastructure, Enterprise, Buildings, Homes and Cities seamlessly. While it is expected to cater to a wide spectrum of applications and deliver multitude of services, it needs to be secure from End-to-End in the entire Signal path and Value chain. Hence, it's imperative for it to be a ***homogeneous & secure paradigm for heterogeneous devices, systems & solutions.***

Creating the opportunity for ecosystem partners to work across common open platforms facilitates faster innovation

Challenges in fast growth of IoT:

- The standards in question are related to the communications nodes and the interactions of these nodes at each segment of this system, from the edge nodes, all the way to the cloud.
- Endless IoT applications - Endless potential types of edge node technologies, and the interface to the communication nodes
- High fragmentation of today's IoT connectivity solutions
- Lots of legacy systems that will now be a part of IPv6 network, with no (or minimal) existing "co-existence" and interoperability plans
- Regulatory issues that will hinder deployments on a worldwide basis
- Slow development of the IoT services market, partially due to lack of future proof standards etc.

The Security aspect of the IoT

- Amidst all the hype and hope of the expected benefits from the Internet of Things (IoT), Security remains its biggest challenge to overcome.
- A smart network is required to maximize the much expected value from IoT, to securely connect thousands of these “things” with the highest levels of security including encryption, authentication, traffic segmentation, intrusion detection and remediation.
- With smartphones posing as a key component of IoT, there is a need to look at the complete lifecycle of the mobile security architecture.
- ***Security and control of identified devices are key aspects in a universe teeming with privacy concerns, insufficient authorization, lack of transport encryption, insecure web interface and inadequate software protection.***

CONCLUSIONS AND RECOMMENDATION

Conclusions & Recommendations

- Convergence of the multitude of stakeholders of the IoT ecosystem to **common standards** is essential for the wide acceptance of the IoT wave by the masses.
- There is an immediate need to develop/adopt standardized frameworks and architectures to bring comprehensive inter-operability in this heterogeneous, diverse and fragmented ecosystem
- It is imperative to standardize a Common Service Layer in the heterogeneous world of M2M/IoT to bring interoperability.
- The key to unified smart infrastructure adoption by the diverse stakeholders shall also lie in the design of the Standards based Gateways (or Data Concentrator Units) with Standardized Common Service Functions.

Conclusions & Recommendations

- In face of the increased vulnerabilities due to the large Attack Surface Area in the M2M/IoT paradigm it's imperative to move from the "EXTRINSIC SECURITY" (Add on Security) paradigm to an "INTRINSIC SECURITY" (Security by Design) paradigm.
- A successful IoT security shall require a multilayered approach to design new systems based on secure software and architectures.
- It would be critical to comprehensively address the challenges created by IoT in the integrity & confidentiality of the data and privacy of an individual.
- A key imperative is creating standards awareness among policy makers, planners, utility suppliers and service providers.
- Harmonization of Policies, Regulations & Standards.

National & Global Co-ordination & Collaboration

- To keep pace with the global developments in Technology & Standards Indian Stakeholders must leverage the initiatives, best practices & work done in Global & Regional SDOs and collaborate closely to speed up the adoption and implementation of required Standards and best practices.

- BIS and TSDSI to work in close collaboration and synchronization; and BIS to adopt the relevant TSDSI deliverables as National Standards.

- MoC, MeitY, TSDSI, BIS and all other ecosystem stakeholders to leverage the initiatives of the **"Project SESEI"** by **EU** and another platform such as "India-EU Cooperation on ICT-Related Standardization, Policy and Legislation" to co-operate and collaborate on areas of mutual interests like M2M/IoT, Security, 5G, NFV/SDN and ensure that Indian stakeholders are technologically at par with global technology advancements.

- Learn from best practices in Standardization, Policies & Regulations from European Union initiatives; and emulate them by constituting High Level Co-ordination groups on important focus areas to harmonize and share the Standardization and other relevant activities in individual National SDO or Industry Bodies.

Study conducted by

- **N. KISHOR NARANG** (Project Lead)
  - Mentor & Principal Design Architect,
  - NARNIX TECHNOLABS PVT. LTD.
- **George Verghese**
  - Former, VP (Telecom), UL MSS India
- **Anupam Kaul**
  - Principal &Head (QMS), CII Institute of Quality

Confederation of Indian Industry

India's leading industry and business association

Policy Advocacy

Thought Leadership

Enhancing Competitiveness

Strategic Global Linkages

Inclusive Development

#EUINStandards

#euroindostandards