Internet of Things: Challenges of IoT

Dr. E.SURESH BABU
Assistant Professor
Computer Science and Engineering Department
National Institute of Technology, Warangal.
Warangal, TS, India.

Session Outline

1. Challenges of IoT
2. Interoperability
3. Standardization
4. Security & Privacy

Internet of Things Communications Models

Rise of the Enabling Technologies

- **Enabling Technologies**
  - ✓ The recent **several technology market trends** is bringing the **Internet of Things** closer to **widespread reality.**
- **Some of the Enabling Technologies**
  - ✓ **Ubiquitous Connectivity,**
  - ✓ **Widespread Adoption of IP-based Networking,**
  - ✓ **Advances in Data Analytics**
  - ✓ **The Rise of Cloud Computing.**

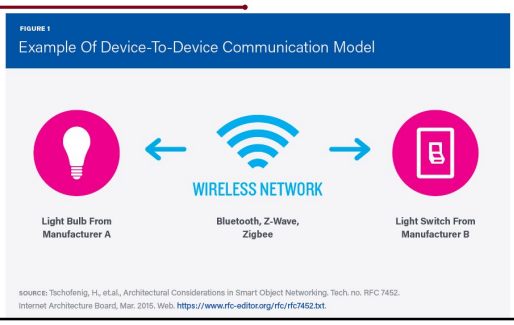
Internet Architecture Board (IAB)

- In March 2015, the **Internet Architecture Board (IAB)** released
  - ✓ **Architectural document** for **networking of smart objects (RFC 7452)**
  - ✓ Outlines a **framework of four common communication models** used by **IoT devices**

IoT Common Communication Models

- **IoT implementations** use **different technical communications models.**
- Each **Model** has its **own characteristics. Four common communications**
  1. **Device-to-Device**
  2. **Device-to-Cloud**
  3. **Device-to-Gateway**
  4. **Back-End Data-Sharing.**

Device-to-Device Communication Model



Device-to-Device Communication Model

- The **device-to-device communication model** represents
  - ✓ **Two or more devices** that **directly connect and communicate** between one another, **rather than** through an **intermediary application server.**
  - ✓ These **devices communicate** over **many types of networks**, including **IP networks or the Internet**.
  - ✓ These **devices** use **protocols** like **Bluetooth Z-Wave or ZigBee** to establish **direct device-to-device communications**, as shown in Figure 1.

Device-to-Device Communication Model

- This **communication model** is commonly used in **applications** like **Home Automation Systems**
  - ✓ Typically uses **small data packets of information** to **communicate between devices** with **relatively low data rate** requirements.
  - ✓ **Residential IoT devices** like **light bulbs, light switches, thermostats**, and **door locks** normally **send small amounts of information** to each other (e.g. a **door lock status message** or **turn on light command**) in a **home automation scenario.**

Interoperability Challenges

- **Interoperability** is the **essential issue** for **crossing layers** of **Physical, Device, Communication Protocol, Function And Application.**
- **Information interoperability**
  - ✓ take place among **Different Things, Different Enterprises, Different Industries, and Different Regions Or Countries.**

Interoperability Challenges

- A **holistic approach** is required in
  - ✓ **Addressing and solving the interoperability of IoT devices**
  - ✓ **Services at several layers.**
- **Transparent Languages** and **Protocols** are Needed
  - ✓ Traditionally, **different languages and protocols** are built on Level and domain

Interoperability Challenges

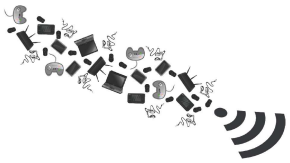
- Devices often use **device-specific data models** that require **redundant development efforts** by device manufacturers.
  - ✓ The **device manufacturers** need to invest in **development efforts** to implement **device-specific data formats** rather than **standard data formats.**

Interoperability Challenges

- **Device-to-device Communication Protocols** are **not compatible**, forcing the **user to select a family of devices** that employ a **common protocol.**
  - ✓ **For example**, the **family of devices** using the **Z-Wave protocol** is **not natively compatible** with the **ZigBee family of devices**.
  - ✓ These **incompatibilities limit user choice** to **devices** within a **particular protocol family**

Interoperability Challenges

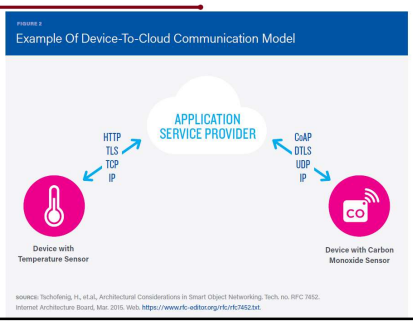
- The **user benefits** from **knowing that products** within a **particular family tend** to **communicate well.**



Interoperability Challenges

- A **holistic approach** is required in
  - ✓ **Addressing and solving the interoperability of IoT devices**
  - ✓ **Services at several layers.**
- **Transparent Languages** and **Protocols** are Needed
  - ✓ Traditionally, **different languages and protocols** are built on Level and domain

Device-to-Cloud Communication Model



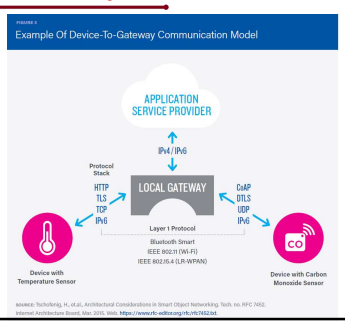
Device-to-Cloud Communication Model

- In a **device-to-cloud communication model,**
  - ✓ The **IoT device** connects **directly to an Internet cloud service**
    - An **application service provider** to **exchange data** and **control message traffic.**

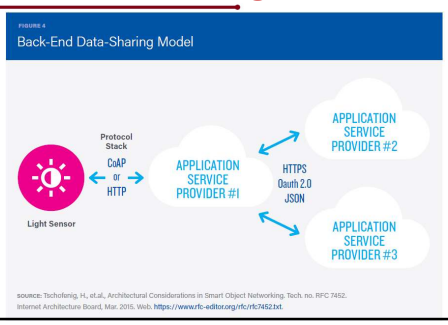
Device-to-Cloud Communication Model

- **Device-to-Cloud approach** frequently takes advantage of **existing communications mechanisms**
  - ✓ Traditional **wired Ethernet or Wi-Fi connections** to establish a **connection between the device** and the **IP network**, which **ultimately connects to the cloud service.**

Device-to-Gateway Model

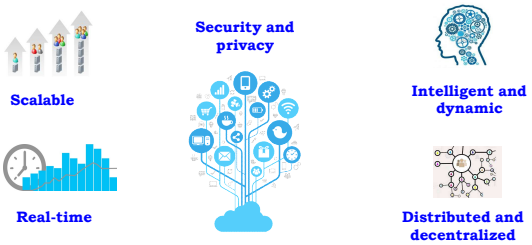


Back-End Data-Sharing Model



Challenges of IoT

Key Requirements of IoT Platform



Open Problems and Challenges

1 Lack of standardization	6 Handling network traffic patterns
2 Scalability	7 Security/Privacy issues
3 Addressing issues	8 Legal, Regulatory and Rights
4 Understanding the big data	9 Emerging Economy and Development Issues
5 Address acquisition	10 Interoperability

Universal Definition

IoT Definitions:

- No Single, Universal Definition.

Architecture Challenge

IoT make use extreme wide range of technologies

- IoT involves an increasing number of **smart interconnected devices and sensors**
- As the communications among all these devices are expected to happen **anytime, anywhere for any related services**
- **Data integrations** over different and **interoperable components** environments are tough
- **Single reference architecture** cannot be a blueprint for all applications.

Architecture Challenge.....

Heterogeneous Reference Architectures have to coexist in IoT.

- Architectures should be open and standards, they should not restrict users to use fixed, end-to-end solutions.

IoT Architectures

- **Flexible** between **intelligent devices**, and **smart objects** (hardware and software solutions).

Technical Challenge

IoT technology can be complex for variety of reasons

- There are **legacy heterogeneous architectures** in the existing networking technologies and applications varies
- Characteristics of **cellular, wireless local area network, and RFID technologies** are much different from each other
- Communication Technologies are either simple or complicated, that should be low cost and with reliable connectivity

Hardware Challenge

IoT provides **High Degrees of Intelligence**

- **Smart devices** with **inter-device communication** will lead to **smart systems**
- Hardware researchers are focusing on **designing wireless identifiable systems** with **low size, low cost yet sufficient functionality.**

Standard Challenge

Standards play an important role in forming IoT

- A standard is essential to allow **all actors to equally access and use.**
- Developments and coordination of standards and proposals will promote efficient development of **IoT infrastructures and applications, services, and devices.**
- Standards developed by cooperated multiparties, and information models and protocols in the standards, shall be open

Standard Challenge

Standards should be open

- The standard development process shall also be open to all participants, and the resulting standards shall be publicly and freely available.
- In today's network world, global standards are typically more relevant than any local agreements.

IoT standard system

The IoT standard system contains

- The Architecture Standards

1. The Application Requirements Standards
2. The Communication Protocol Standards
3. The Identification Standards
4. The Security Standards
5. The Application Standards
6. The Data Standards
7. The Information Processing Standards
8. The Public Service Platform Standards

Companies involved in IoT Standardization

Open Interconnect Consortium

- **Atmell, Dell, Intel, Samsung and Wind River**

Industrial Internet Consortium

- **Intel, Cisco, GE, IBM**

Open Connectivity Foundation (OCF)

- **Intel, Samsung, Microsoft, Electronux, Qualcomm, Cisco**

Intelligent System

The IoT brings

- Seamless business and social networking over fast reliable and secure networks into our society

System Intelligence

- **System intelligence** will be important for the **development of IoT** and key point in **inter-things information exchange**

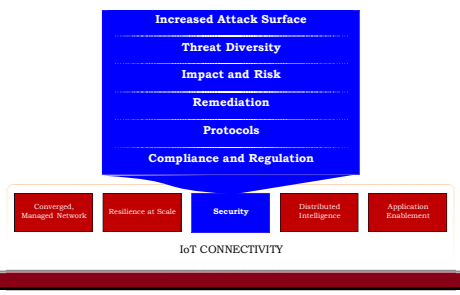
Intelligent System

Focus of Research

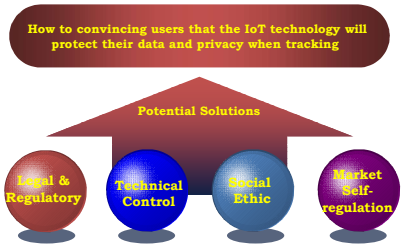
- Increase and adapting the **intelligence at the device level** will be a focus of research
- Integration of sensors and actuators, high efficiency, multi-standard and adaptive communication subsystems, and adaptable antennae.

Security

IoT Expands Security Needs



The Security Challenge of IoT



Security Must Be A Fundamental Priority

Important IoT Challenge

- **Security** is the most pressing and important IoT challenge for **industry, users, and the Internet.**

Top Priority For The Sector

- **Ensuring security** in **IoT products and services** should be considered a **top priority for the sector.**

Security Must Be A Fundamental Priority

Cyber Attack

- Growth in devices increases the surface available for **cyber attack**

Affect

- **Poorly secured devices** affect the **security of the Internet** and other **devices globally**, not just **locally.**

For Example

- An **unprotected refrigerator or television** that is **infected with malware** might send **thousands of harmful spam emails** to recipients worldwide using the **owner's home Wi-Fi Internet connection**

The IoT Security Challenge

Security in IoT

- Security in IoT is fundamentally linked to the ability of users to **trust their environment.**

Believe in IoT

- If people **don't believe** their connected devices and their information are reasonably **secure from misuse or harm**, the resulting **loss of trust** causes a reluctance to use the Internet.

The IoT Security Challenge

Critical Issue

- **Security of IoT** devices and services is a **major discussion point** and should be considered a **critical issue**

Unique Smart Object Security Challenges

- **Cost/Size/Functionality**
- **Volume of Identical Devices**
- **Deployment at Mass Scale**
- **Long Service Life**
- **No / Limited Upgradability**
- **Limited Visibility into Internal Workings**
- **Embedded Devices**
- **Physical Security Vulnerabilities**
- **Unintended Use**

Privacy

Privacy Challenge

Individual Privacy

- The full potential of the IoT depends on **strategies that respect individual privacy choices** across a **broad range of expectations**

Privacy And Potential Harms

- Privacy and potential harms might hold back **full adoption of the Internet of Things.**

Privacy Challenge

Privacy Rights And Respect

- **User privacy expectations** are integral to ensuring **user trust and confidence** in the **Internet, connected devices, and related services.**

IoT Privacy Questions

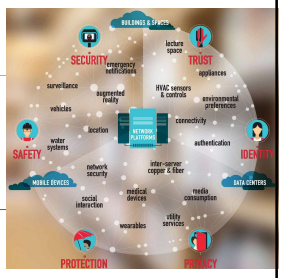
1. Fairness in Data Collection and Use.
2. Transparency, Expression, and Enforcement of Privacy Preferences.
3. Wide-Ranging Privacy Expectations.
4. Privacy by Design.
5. Identification.

Issues of IoT

- Currently, IoT itself lacks
  - ✓ **Theory,**
  - ✓ **Technology Architecture,** and
  - ✓ **Standards**
- Integrate the **virtual world** and the **real physical world** in a unified framework

Success of IoT

- **Trust**: Allow only designated people/services device or data access
- **Identity**: Validate the identity of people, services, and "things"
- **Privacy**: Ensure device, personal & sensitive data is kept private
- **Protection**: Protect devices and users from harm
- **Safety**: Provide safety for devices, infrastructure and people
- **Security**: Maintain security of data, devices, people, etc.



Thank U