Internet of Things (IoT)

Dr.V.N.Sastry

Professor

Centre for Mobile Banking (CMB)

5G Use Case Lab for BFS

Institute for Development and Research in Banking Technology (IDRBT), Hyderabad

Chairman, Working Group on Mobile Device Security, MEITY, GoI

Chairman, Expert Committee on m-Governance, MEITY, GoI

Co-founder & Exec. Secy, Mobile Payment Forum of India (MPFI)

E-Mail : vnsastry@idrbt.ac.in Ph: 91-40-23294304

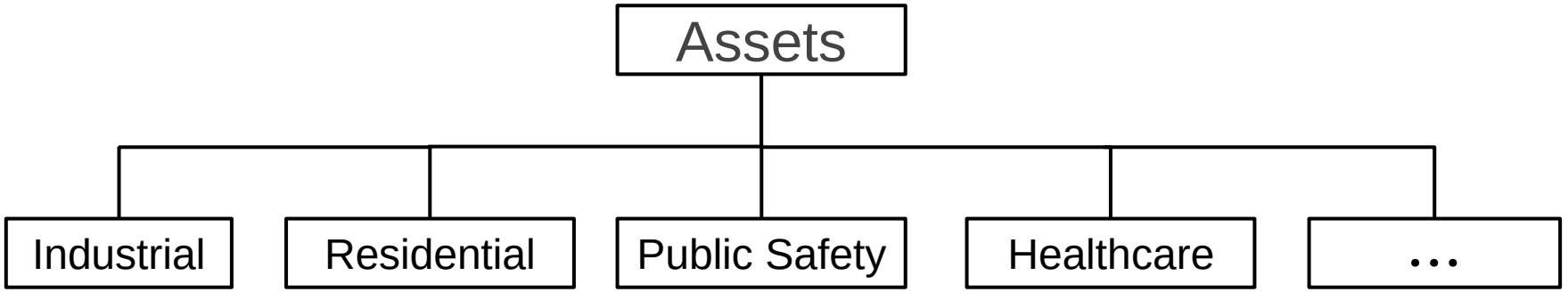
Outline

- Basics of IoT
- Standards
- Applications
- Challenges
- Security

Internet of Things (IoT)

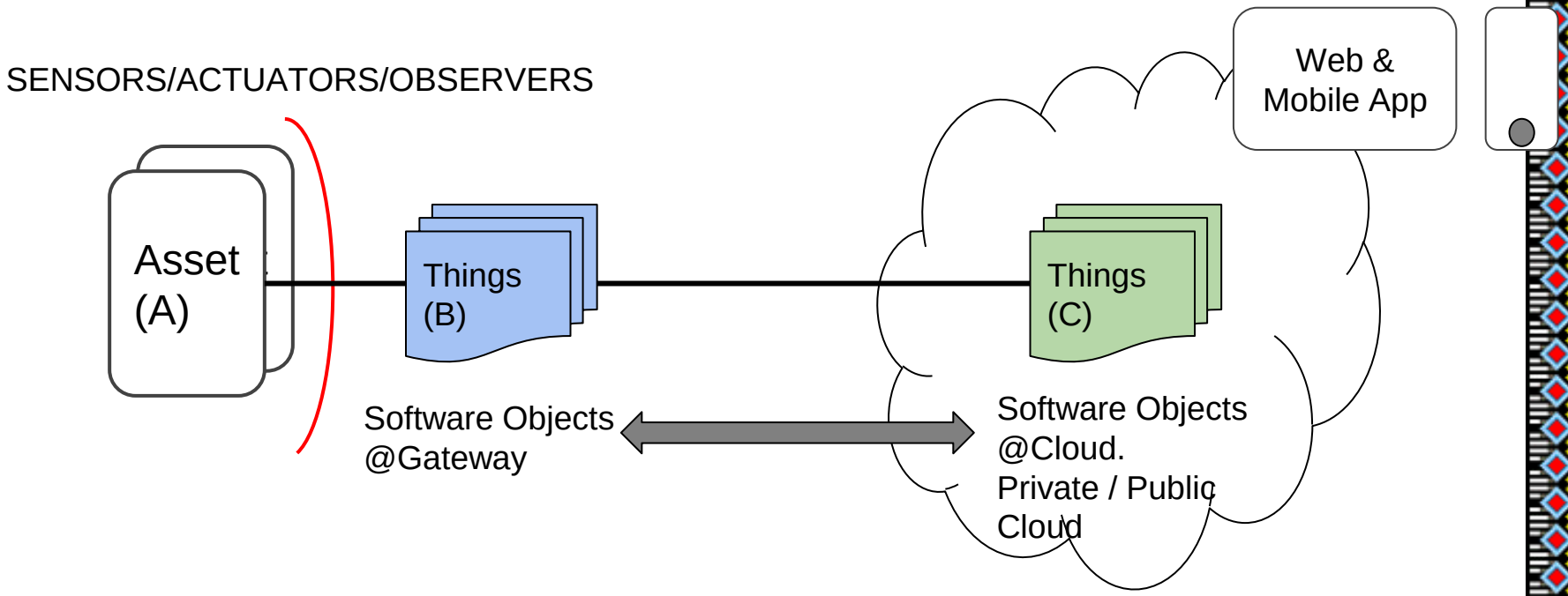
- Every Computing Device has
  - Hardware, Software and Firmware
- Some Digital Devices have computing and Communication capabilities
- IoT are digital devices having computing, communication and sensing capabilities and connected to Internet
- Smart Devices have capability to take decisions as per its embedded intelligence
- IoT Devices form Wireless Sensor Networks

Asset Overview



- Businesses manage “Assets” and create value, it is very obvious that those “Assets” are “THINGS” of IoT
- IoT is applicable to all business where “ASSETS” are connected.

Asset ⇒ Thing



- Assets {A} are now connected AS {B} at the Edge and AS {C} in the cloud.
- This is the crux of IoT designs. Once the software objects of Assets are present in the “Compute and Network”, environment, it opens doors of “Connected” Apps.

Mobile Phone (A Smart IoT Device) has

- Power Section
  - Power Charging & distribution
- Radio Section
  - Signaling (A/D & D/A), Band Switching, RF Power Amplification
  - Transmitter & Receiver Antennas
- Computing Section
  - CPU, Memory (RAM,FLASH,COMBO CHIP)
  - Storage (Micro SD Card, Hard Disc)
- Service Section
  - OS, Applications
- Sensing Section
- Interface Section

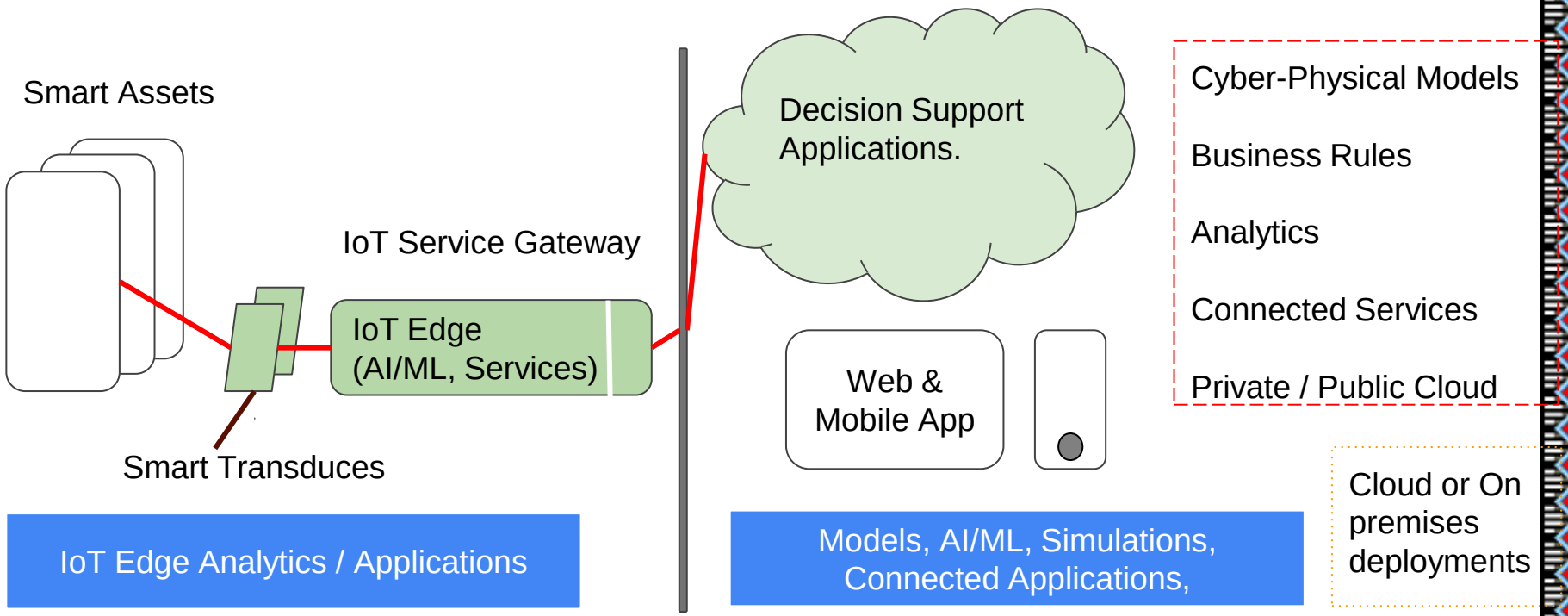
SIM Card

- A SIM card is a Subscriber Identity Module application on a smartcard that stores data for GSM Cellular telephone subscribers
- SIM is smart card with a processor, OS, non volatile memory.
- SIM Card is useful for identification of the customer, authentication of the customer, Storage like contacts, Operator approved limited applications of low capacity.
- Standard smart card reader in the mobile device has SIM access software to access the data stored in binary form in the SIM.
- It does not have its own power.
- SIM cards are transferable between different mobile devices.
- It stores the IMSI Number for Subscriber authentication.
- USIM is Universal SIM which is on UICC (Universal Integrated Circuit Card) and has Secure Element.

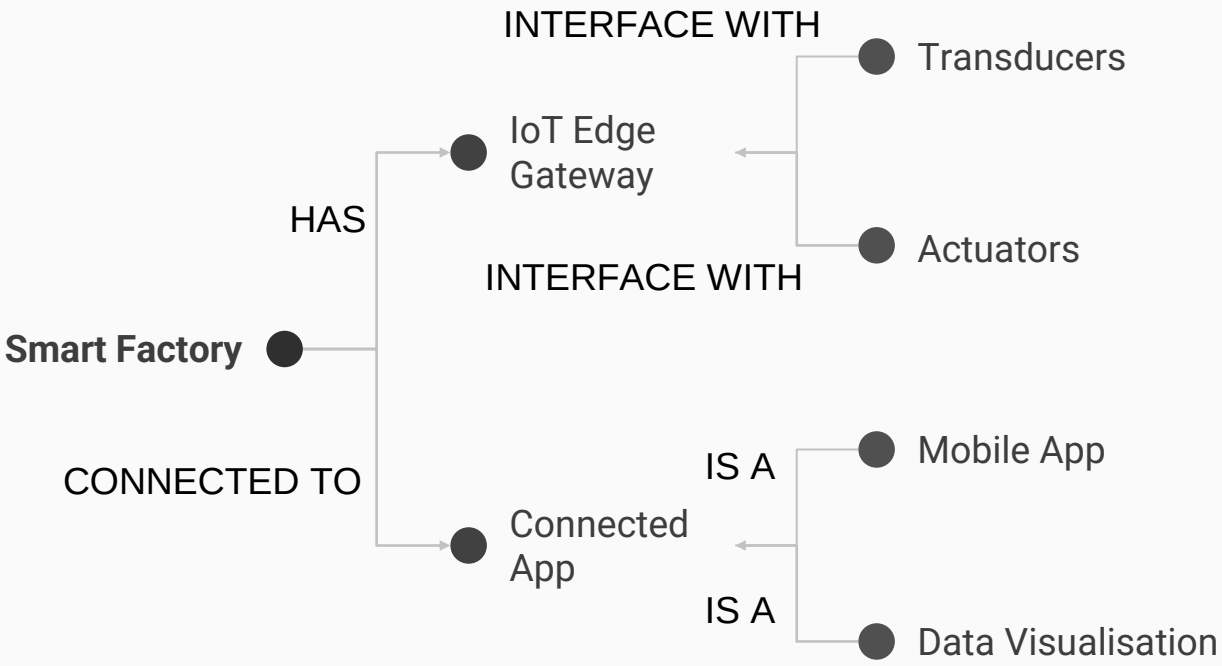
Popular Sensors

- **Motion Sensors**
  - **Accelerometer, gyroscope**
- **Environmental Sensors**
  - **Light, Proximity, Temperature**
- **Position Sensors**
  - **Audio, Camera, Barometer, Heart Rate**
  - **GPS, Magnetic Sensor**

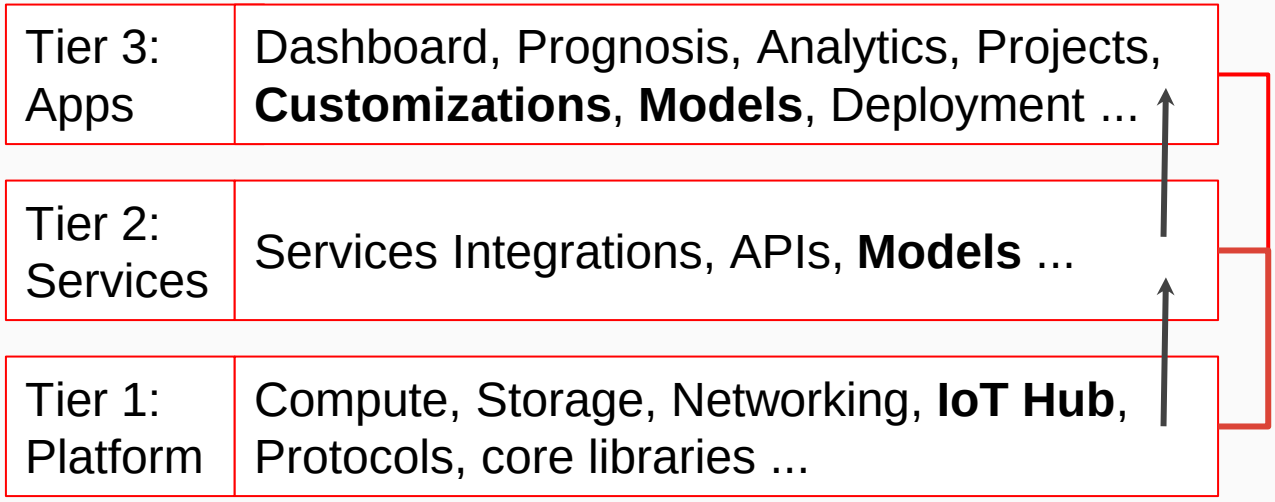
IoT Edge Systems Overview



Industrial IoT Architecture



The Platform Model



Tier 1, 2 are core platform offerings. Tier 3 (Apps) is a service layer.

The Platform Model contd...

- Runs on SBC such as Raspberry Pi, Beaglebone etc.
- Interfaces with Transducer Boards (Anybus Communicators, Texas Instruments, Arduino, Custom Boards)
- Supports variety of communication protocols
- Portable Storage for Transducer data (millions of data points at the gateway).

The Platform Model contd...

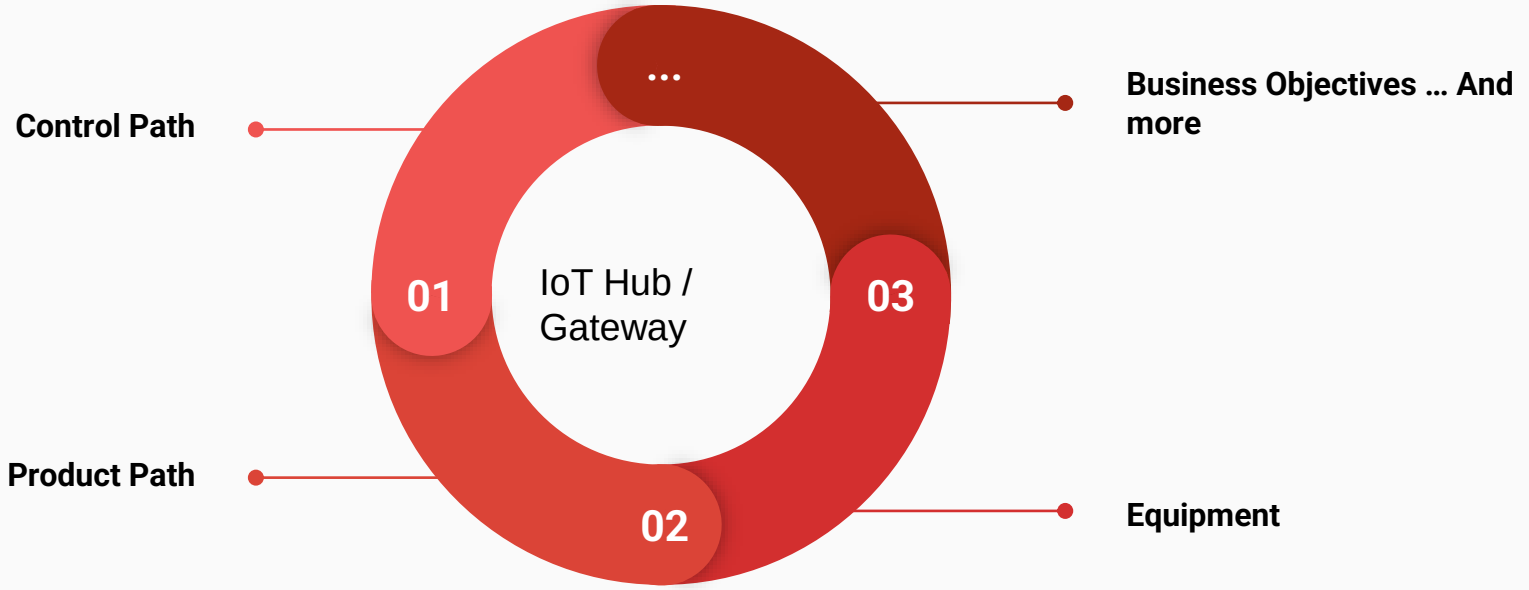
- Runs OPC client to connect any existing Automation infrastructure.
- Supports variety of networking protocols to connect to the cloud applications.
  - HTTP, CoAP, Websockets, MQTT, XMPP, AMQP, ZeroMQ
- Development in C/C++, Python, JavaScript...
- Modular designs for Transducer interfaces.
- Alarm Management

The Platform Model contd...

Models and Processing at the Edge IoT Gateway:

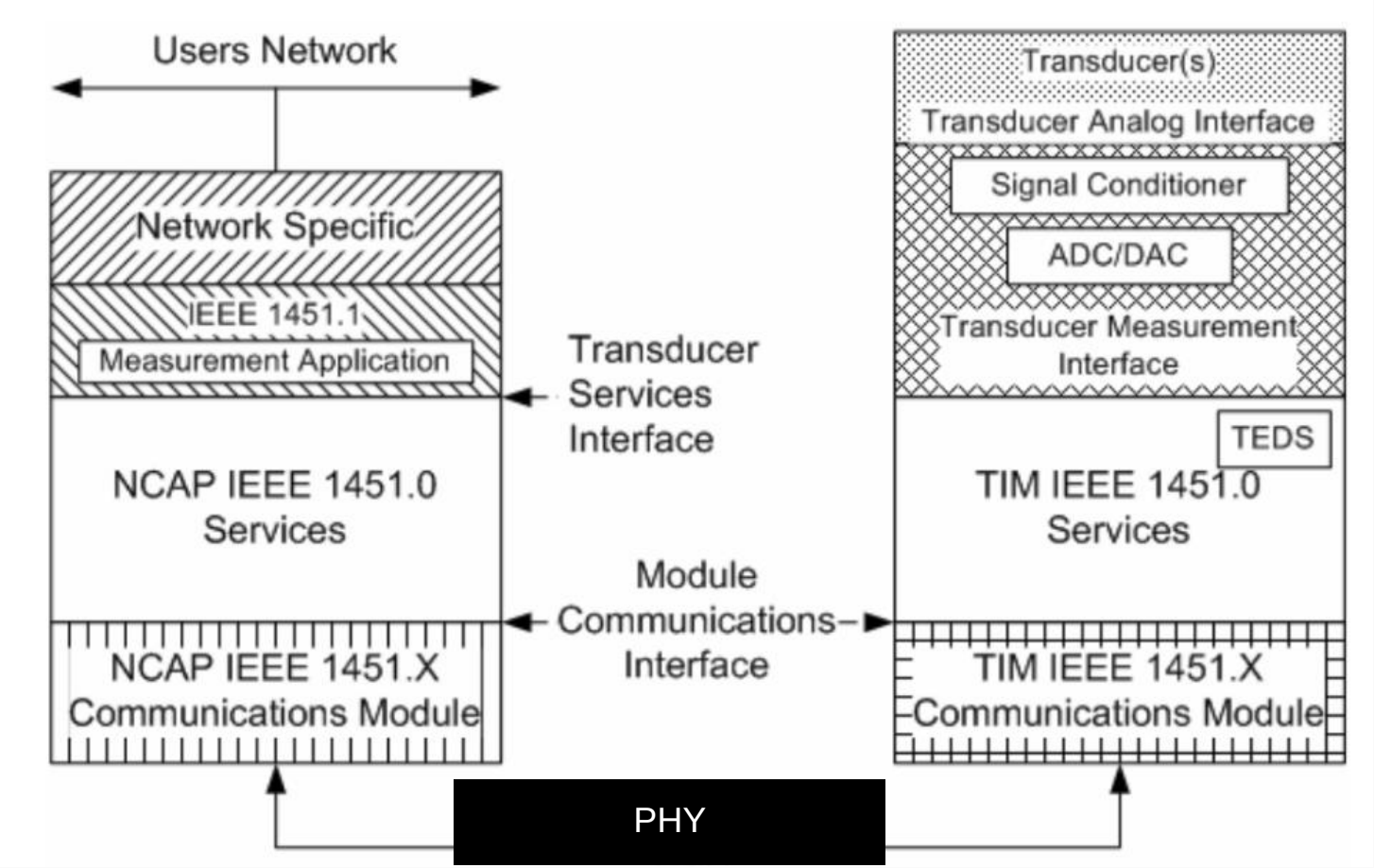
- Ability to process data at the Edge.
- Statistical analysis on transducer data at the Edge.
- Scalable gateway architecture - adding additional gateway units for more compute power.
- Bidirectional communication - Cloud <> Gateway (for decision events)

The Industrial IoT Edge System (Picominer offers)



- IoT is a new channel to observe and control the assets
- IoT is NOT a replacement of Automation (Yet!).
- IoT augments the present day industrial technologies enabling “Things” (Digital Twins)

Let's take a look at the 1451 Standard contd...

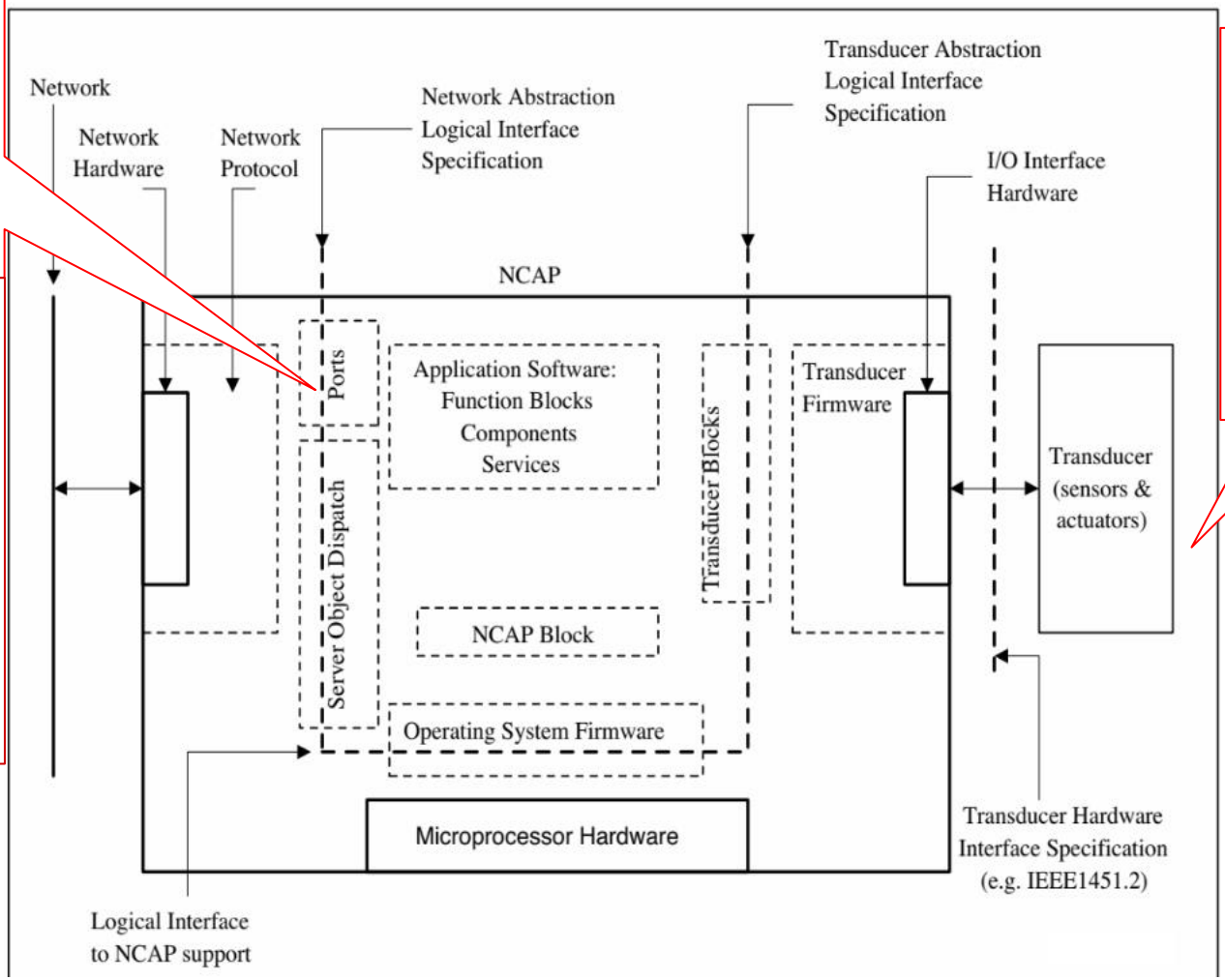


View of the 21451 NCAP Interfaces

Things (AI/ML models at the Edge)

1. Realtime Edge Analytics
2. MES at the Edge
3. Safety
4. Security
5. OPC-UA client

.. etc.



TEDS Transducer Electronic Data Sheets (=> Data Models of Transducers)

Classification of IoT Applications

1st Generation	2nd Generation	3rd Generation	4th Generation
Simple applications	Brownfield Apps	Smart Factories	Industry 4.0
Fun, Learning	E.g. Agriculture	Connected Applications	Truly Digital Transformation.
		...	Very exciting future with a new form of economy.

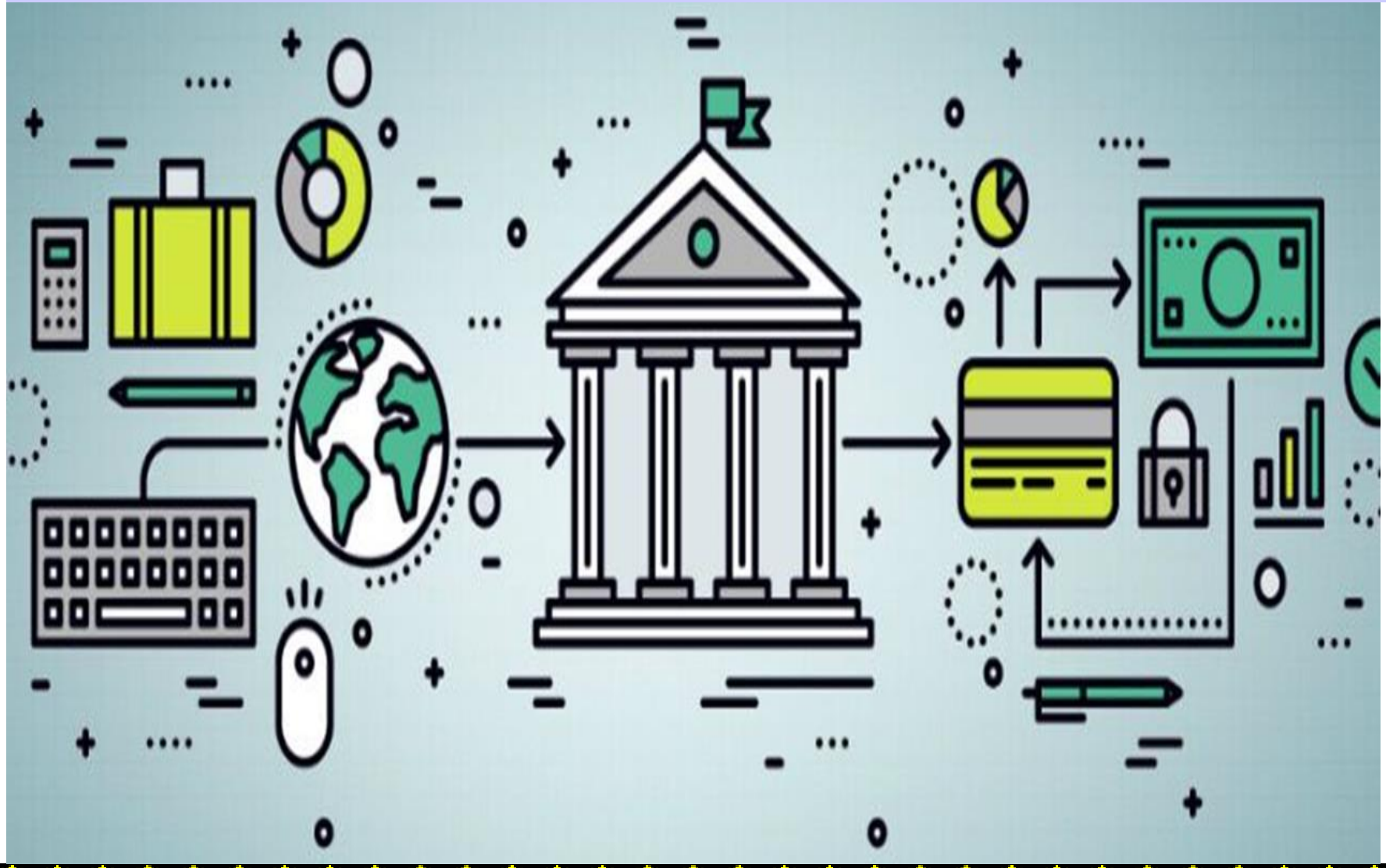
IoT Applications

- Smart Metering (Electricity, Water, Gas, Drainage etc.)
- Video Surveillance, Airport traffic management
- Indoor and Street Lightening
- Smart Home, Building and Wi-Fi connected devices
- Wearable Devices and Patients Health Parameters Monitoring by Doctor remotely
- Drone based Crop and Cattle monitoring
- Industrial IoT in Manufacturing, Robotic Automation, Logistics and Supply Chain
- Digital India Mission Mode Projects in various sectors (NeGD)

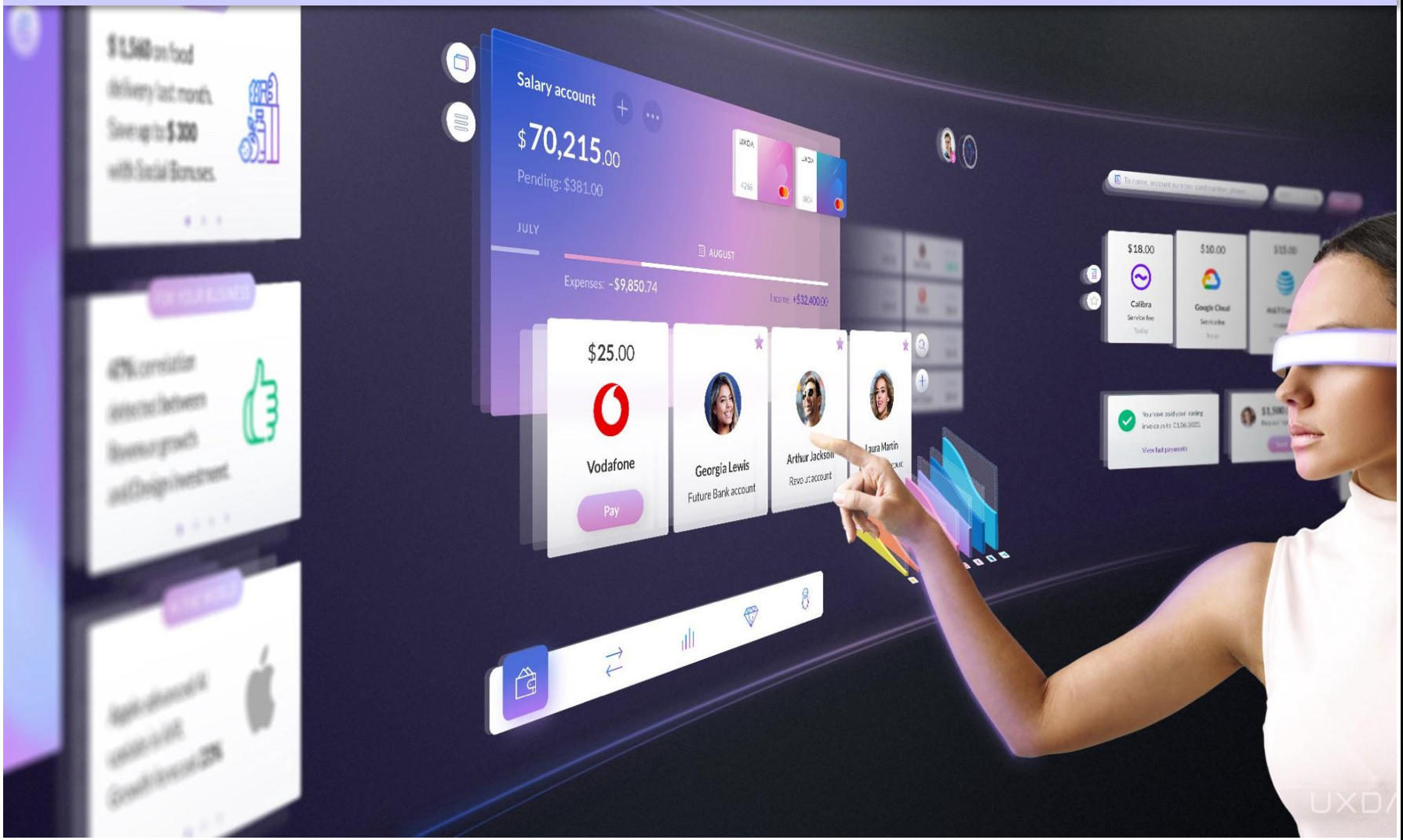
IoT Applications Contd..

- Smart ATM, Bank Branch, Data Centre
- NFC, UPI, QR Code and Fast-tag Payments
- Safe Landing of Aero planes
- Intrusion and Fraud Detection
- Location Tracking
- Weather, Temperature and Pollution Monitoring
- Cyclone, Earth Quake, Infiltration Warning and Sending Alerts
- Routing of Vehicles to Park at Available Free space

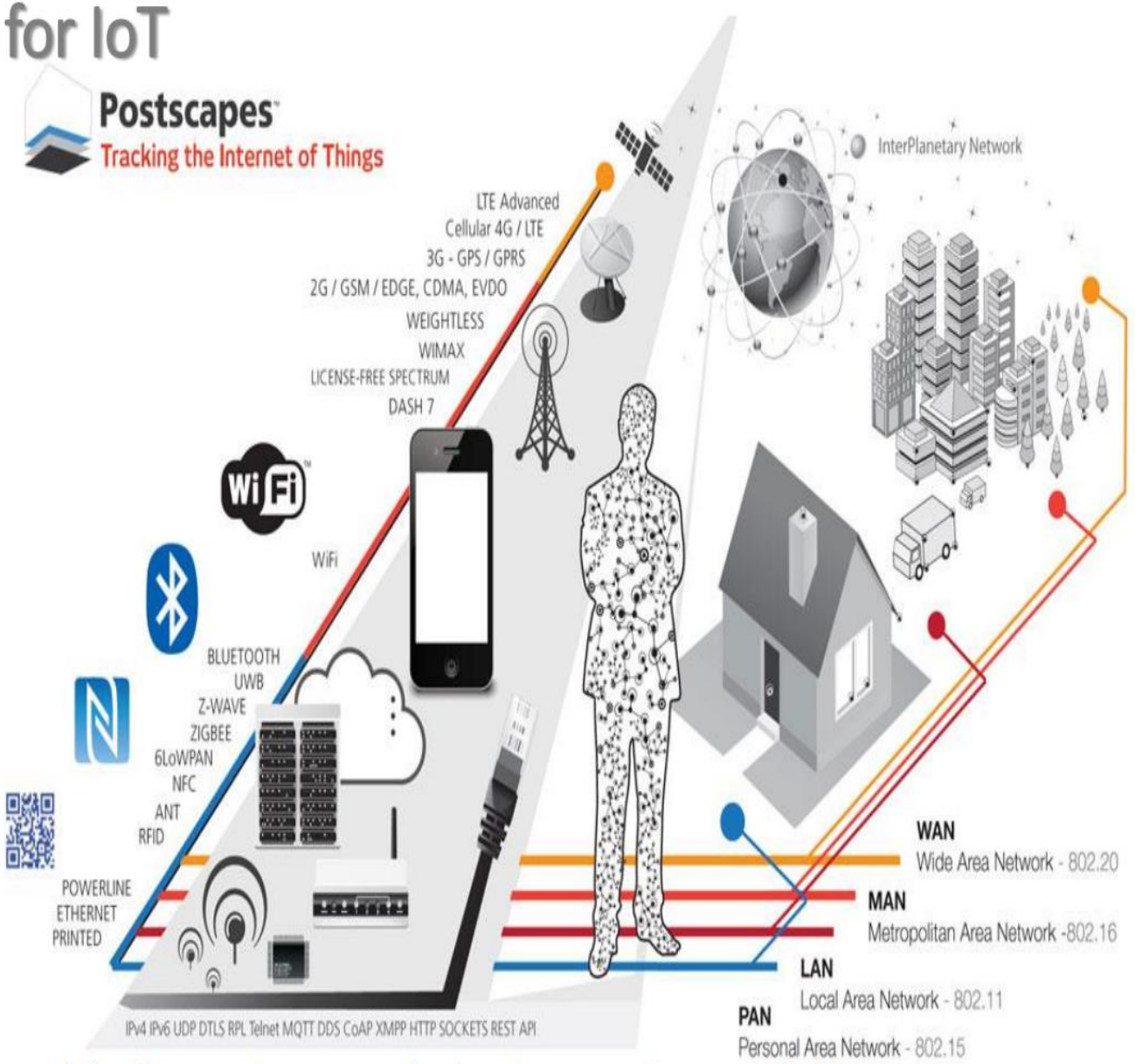
IoT for Banking



Virtual Reality and Augmented Reality



Connectivity for IoT



https://www.postscapes.com/reviews-tag-presenttags-overview/

IoT Challenges

- Deployment
- Energy Supply
- Monitoring
- Data Privacy
- Security
- Device authentication
- Certified Devices
- Interoperability
- Scalability of connected devices
- Cyber attacks
- Regulations
- NB-IoT, Cellular IoT
- UAV etc.

Challenges of Exposing to Internet

WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.

WINDOWS PCs | MACS | ANDROID TABLETS | SMART PHONES

Passwords
- Web browser autofill
- Stored in the file system

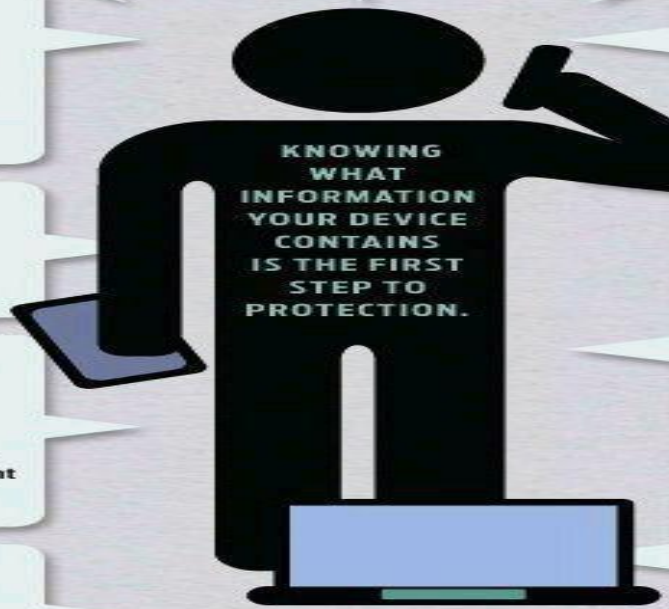
Credit Card Numbers
- Web browser autofill
- Downloaded credit card statements

Social Security Number
- Downloaded tax documents

Deleted Files
- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages
- Text log stored on phone

Phone Calls
- Call log stored on phone



Bank Account Info
- Downloaded bank statements

Name and Address
- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

Recent Files
- List kept by operating system
- Various applications keep their own recent file lists

Recently Visited Sites
- Browser's cache
- Browser's history
- Cookies

Contacts
- Windows Contacts
- Address Book
- Contact manager

Current Location
- Readable off your GPS

Recent Locations
- Photos
- Navigation apps

CYBER CRIME STATISTICS

Average monetary cost to victim of cyber crime:

$128

Email scams sent daily:

75 MILLION

Daily victims of scam emails:

2,000

Percent of Americans who have experienced cyber crime:

73%

Percentage of Americans who believe that cyber-criminals will not be brought to justice:

78%

Percentage of Americans who expect to escape cyber crime in their lifetime:

2%

SOURCE: CYBER CRIME WATCH

Threats and Vulnerabilities

- **Threats arise due to existence of exploitable vulnerabilities in an entity or system.**
- **Identification of the mobile security vulnerabilities is necessary to plug and insulate them from attackers.**
- **Control Measures of Mobile Security**
  - **Generic Measures**
  - **User Specific Measures**
  - **Technology Oriented Measures**

Security Goals

Security Goals	Meaning	Enabling Techniques
Confidentiality	Ensures that critical or transaction information remains secret and cannot be known or viewed by unauthorized persons.	Hiding and Coding, Encryption & Decryption
Integrity	Ensures that the original message or information remains intact without any modification, tampering or alteration at stored or during transit.	Hash Function, Permission Control
Availability	Ensures that services or resources are made available for access from anywhere and anytime.	Security Policy and Administration
Authentication	Ensures that the claiming entity is verified as registered or original entity.	User, Device, Channel, Application and Transaction are to be authenticated. User is verified by 3 factors: Knowledge (like PIN), Possession (like mobile phone or Card) and intrinsic property (as biometrics).
Authorization	Ensures that an authenticated entity uses only the privileged and permitted resources and is controlled from using any unauthorized resources.	Permission Control and Monitoring

Security Goals Contd..

Security Goal	Meaning	Enabling Techniques
Non-repudiation	Property that ensures that no one should be able to claim that the transaction on his/her behalf was made without their knowledge.	Digital certificates & Digital signatures
Reliability	Property that ensures that an entity (path, service, system, user) is reliable.	Trust and Behavior Analysis, Transparency, Scenario and Stress Testing.
Access Control	Property that ensures that genuine entity is not denied access to a privileged service and unauthorized or impersonating entity is not allowed any access.	Access Control Models (DAC, MAC, RBAC, Fine Grained AC etc.), Firewalls, IDS, DMZ.
Traceability	Property that ensures that the original path traversed for the completion of a transaction is traceable and is identified as genuine.	Tracing the source, destination and intermediate nodes by position, time, status logs as proof of evidence.
Trust	Property that ensures that the participating entity is trust worthy.	Statistical Analysis on adherence and violation of rules.

THANK YOU