Course Name:
IoT & Applications

Class-2

Module-2: **IoT Strategies-** Adaptive & Event Driven Processes, Virtual Sensors, Security, Privacy & Trust, Low power communication, Energy harvesting, IoT related standardization

IoT Strategies

- The deployment of IoT technologies will significantly impact and change the way enterprises do business as well as interactions between different parts of the society, affecting many processes.
- To acquire the potential benefits that have been postulated for the IoT, several challenges regarding the modelling and execution of such processes need to be solved in order to see wider and in particular commercial deployments of IoT.
- The special characteristics of IoT services and processes have to be taken into account.

Adaptive and Event-Driven Processes

Virtual Sensors

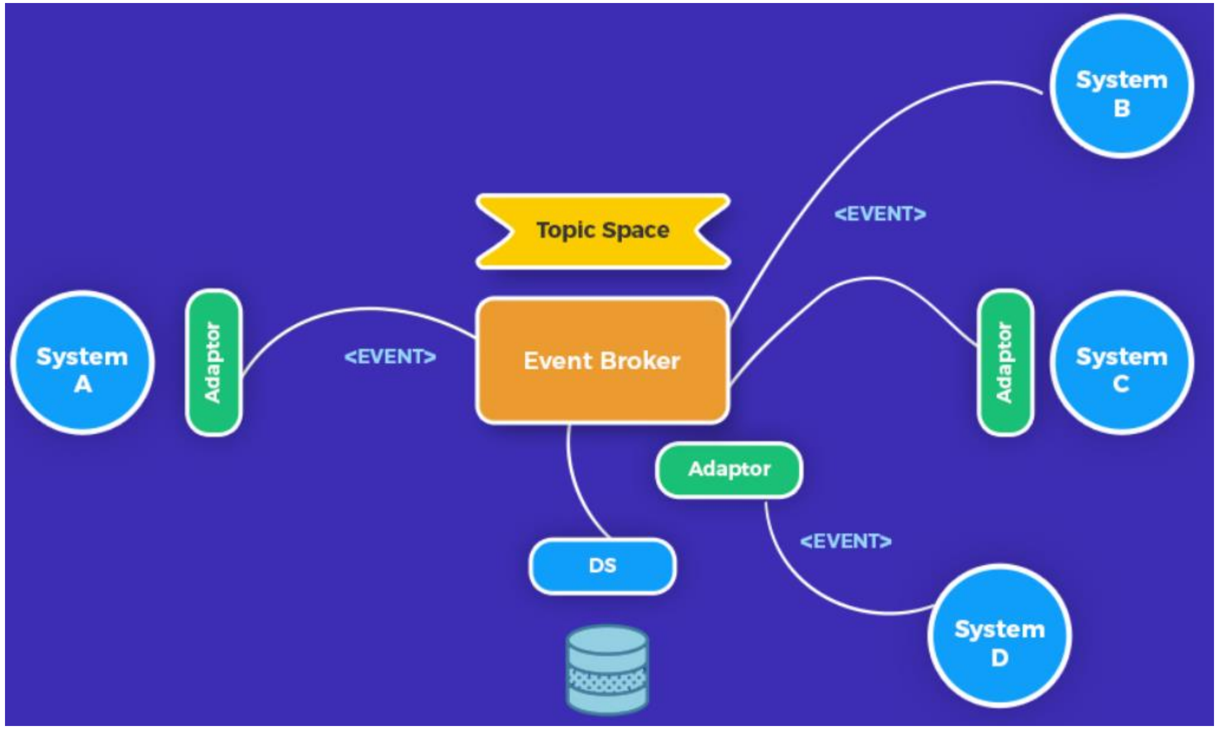
Security, Privacy &Trust

Adaptive and Event-Driven Processes

- One of the main benefits of IoT integration is that processes become more adaptive to what is actually happening in the real world.
- Inherently, this is based on events that are either detected directly or by real-time analysis of sensor data. Such events can occur at any time in the process.
- For some of the events, the occurrence probability is very low: one knows that they might occur, but not when or if at all.
- Modelling such events into a process is cumbersome, as they would have to be included into all possible activities, leading to additional complexity and making it more difficult to understand the modelled process, in particular the main flow of the process.
- Secondly, how to react to a single event can depend on the context, i.e. the set of events that have been detected previously.

Adaptive and Event-Driven Processes --- Cont…

- Research on adaptive and event-driven processes could consider the extension and exploitation of EDA (Event Driven Architectures) for activity monitoring and complex event processing (CEP) in IoT systems.
- EDA could be combined with business process execution languages in order to trigger specific steps or parts of a business process.



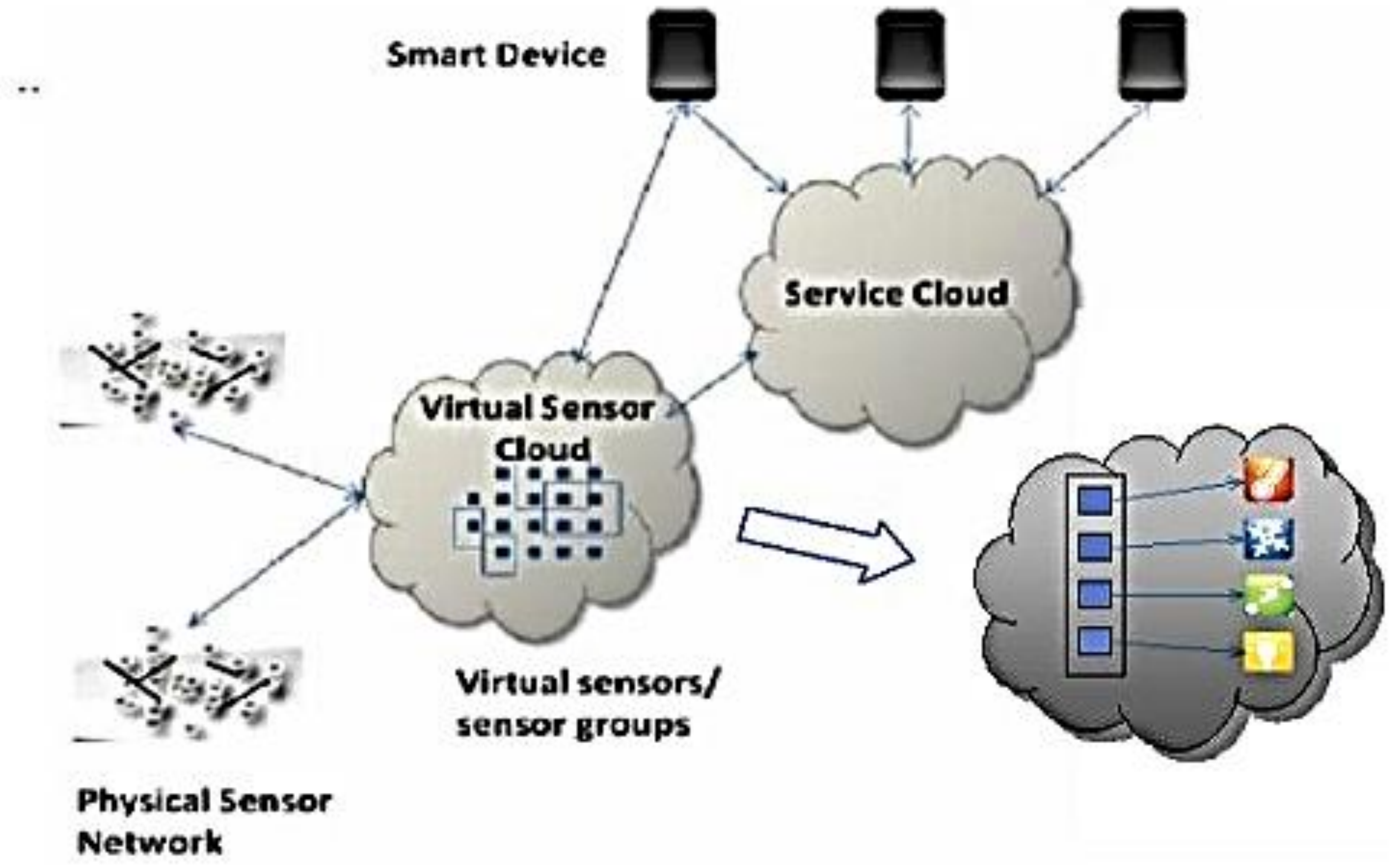
Virtual Sensors

- A virtual sensor can be considered as a product of spatial, temporal and/or thematic transformation of raw or other virtual sensor producing data with necessary source information attached to this transformation.
- Virtual sensors and actuators are a programming abstraction simplifying the development of decentralized WSN applications.
- Models for interacting with wireless sensors such as Internet of Things and sensor cloud aim to overcome restricted resources and efficiency.

Virtual Sensors

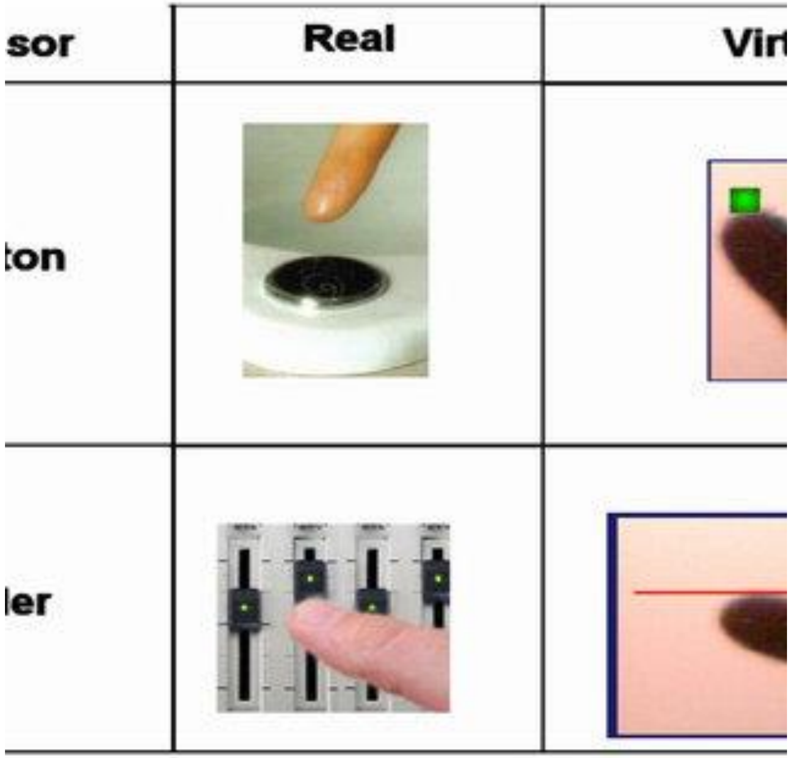
- New sensor clouds need to enable different networks, cover a large geographical area, connect together and be used simultaneously by multiple users on demand.
- Virtual sensors, as the core of the sensor cloud architecture, assist in creating a multiuser environment on top of resource constrained physical wireless sensors and can help in supporting multiple applications.

Virtual Sensors --- Cont…



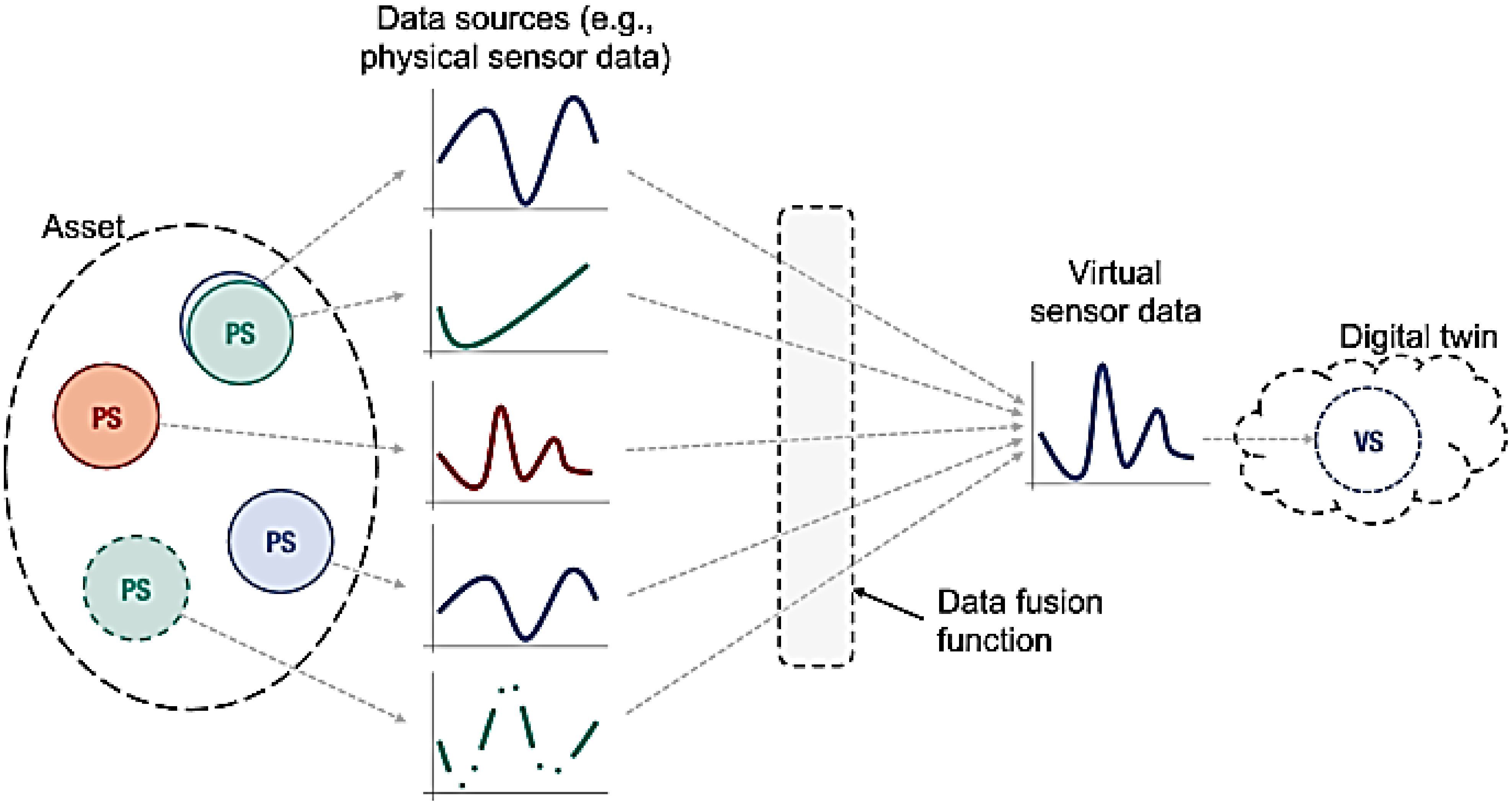
virtual-sensor

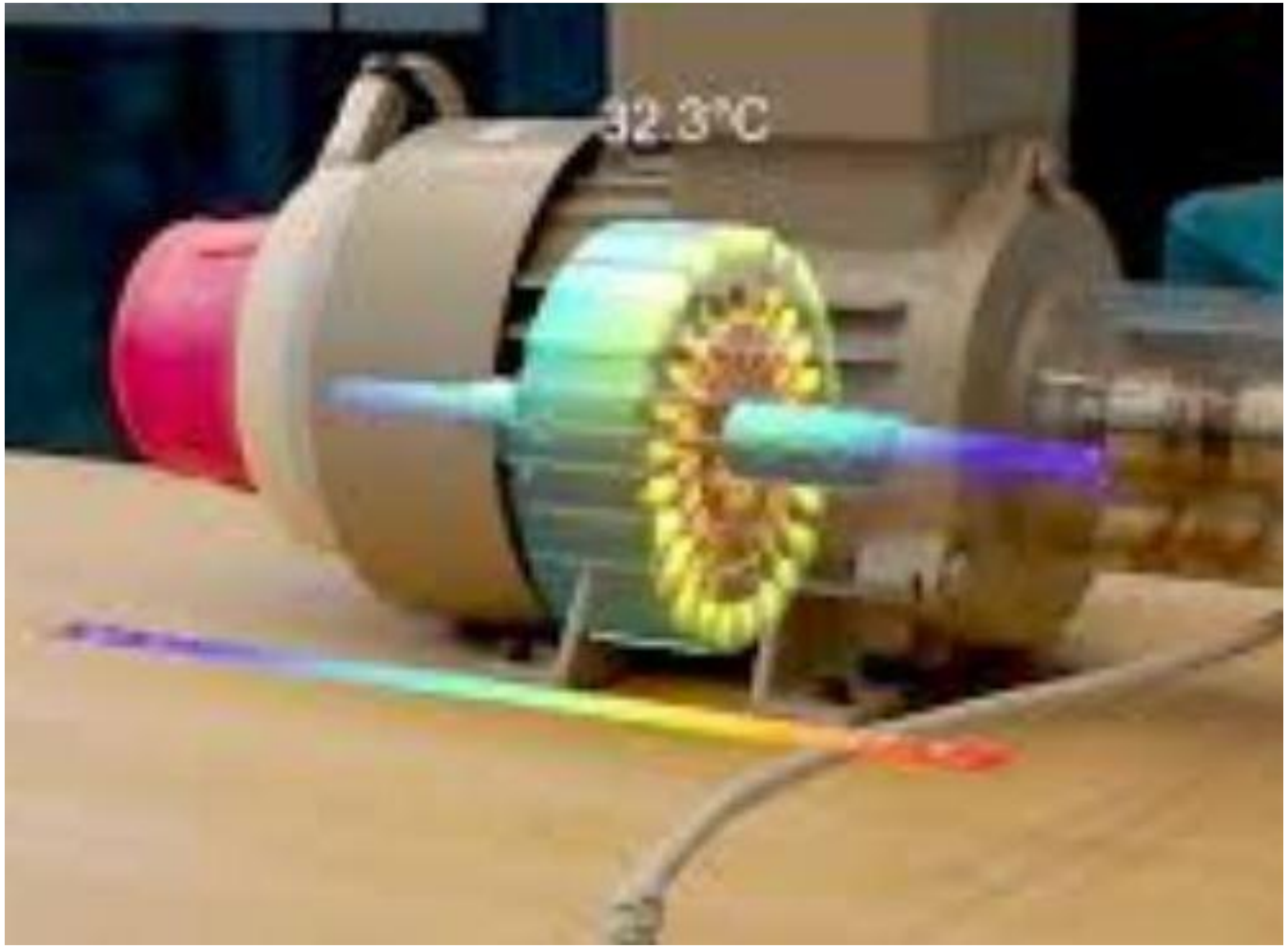
Example



sor	Real	Vir
ton		
ler		

Virtual Sensors --- Cont…

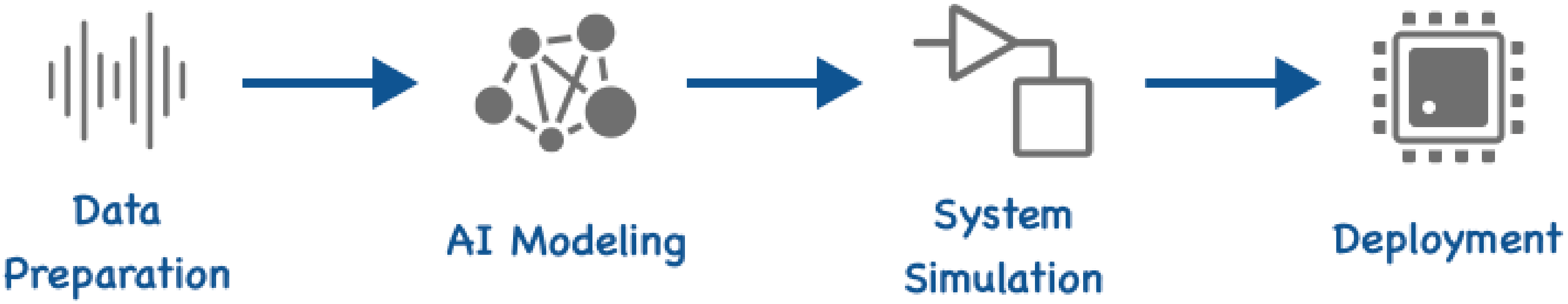



32.3°C

Virtual Sensors --- Cont…

- The data acquired by a set of sensors can be collected, processed according to an application-provided aggregation function, and then perceived as the reading of a single virtual sensor.
- A virtual sensor behaves just like a real sensor, emitting time-series data from a specified geographic region with newly defined thematic concepts or observations which the real sensors may not have.
- A virtual sensor may not have any real sensor’s physical properties such as manufacturer or battery power information, but does have other properties, such as: who created it; what methods are used, and what original sensors it is based on.

Workflow: Virtual Sensors Using AI



Security, Privacy &Trust

- There are a number of specific **security, privacy and trust challenges in the IoT**,
  - Lightweight and symmetric solutions, Support for resource constrained devices.
  - Scalable to billions of devices/transactions.
- Solutions will need to address federation/administrative co-operation
  - Heterogeneity and multiplicity of devices and platforms.
  - Intuitively usable solutions, seamlessly integrated into the real world.

Security, Privacy &Trust --- Cont…

- As IoT-scale applications and services will scale over **multiple administrative domains and involve multiple ownership regimes**, there is a need for a **trust framework** to enable the **users** of the system to have confidence that the **information and services** being **exchanged** can indeed be **relied** upon.
- The trust framework needs to be able to deal with **humans and machines as users**, i.e. it needs to convey trust to humans and needs to be **robust** enough to be used by machines without denial of service.

Security, Privacy &Trust --- Cont…

- The development of trust frameworks that address this requirement will require advances in areas such as:
  - **Light weight Public Key Infrastructures (PKI)** as a basis for trust management.
  - There are **two basic types of cryptographic algorithms**: symmetric, or private key, and asymmetric, or public key.
  - Advances are expected in hierarchical and cross certification concepts to enable solutions to address the scalability requirements.

Security, Privacy &Trust --- Cont…

- **Lightweight key management systems** to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources, as is consistent with the resource constrained nature of many IoT devices.
- **Quality of Information** is a requirement for many IoT-based systems where **metadata can be used** to provide an assessment of the reliability of IoT data.

Security, Privacy &Trust --- Cont…

- **Decentralized and self-configuring systems as alternatives to PKI** for establishing trust e.g. identity federation, peer to peer.
- Novel methods for assessing trust in people, devices and data, beyond reputation systems. One example is **Trust Negotiation**.
- **Trust Negotiation** is a mechanism that allows two parties to automatically negotiate, on the basis of a chain of trust policies, the minimum level of trust required to grant access to a service or to a piece of information.

Security, Privacy &Trust --- Cont…

- Assurance methods for trusted platforms including hardware, software, protocols, etc.
- Access Control to prevent data breaches.
- One example is Usage Control, which is the process of ensuring the correct usage of certain information according to a predefined policy after the access to information is granted.

Security for IoT

- As the IoT becomes a key element of the Future Internet and a critical national/international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important.
- **Large-scale applications and services based on the IoT are increasingly unsafe to disruption from attack or information theft.**

Contd.

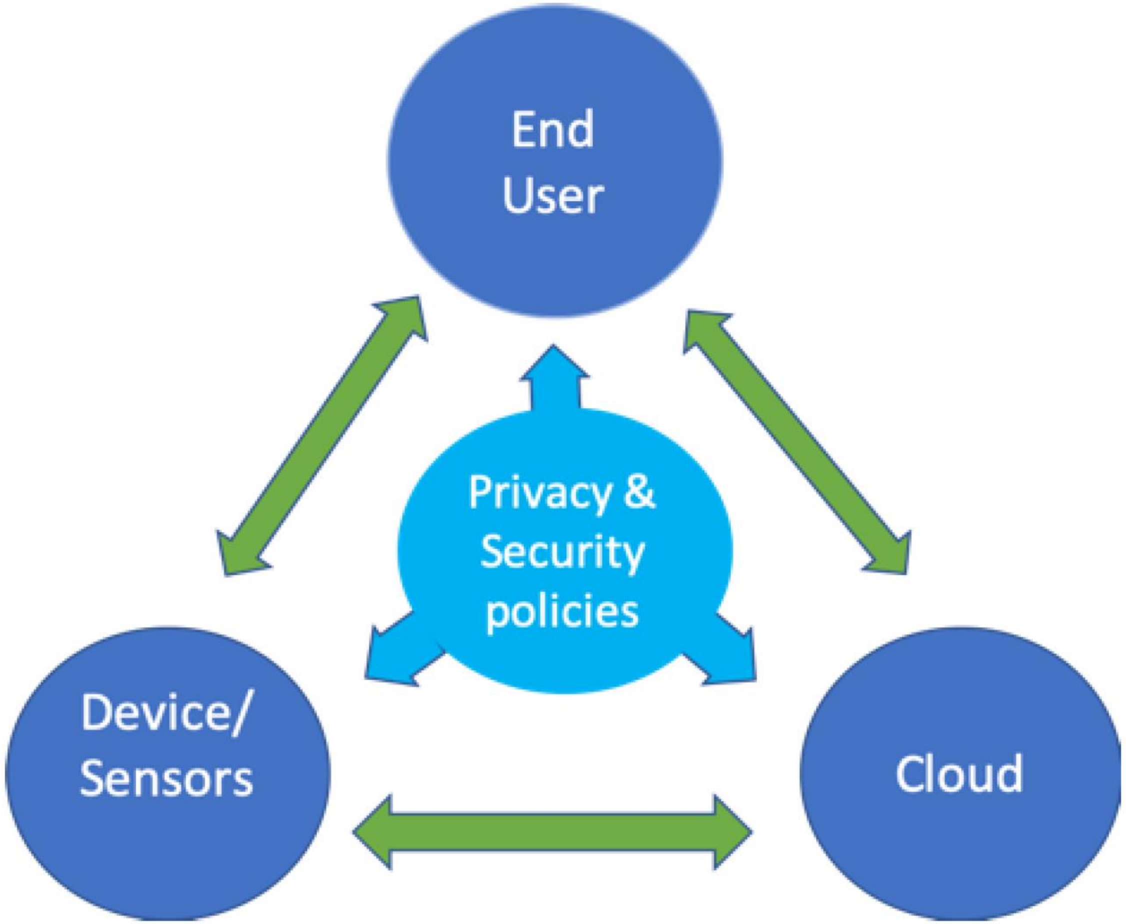
- Advances are required in several areas to make the IoT secure from those with malicious intent, including
  - IoT is always susceptible to the well-known **DoS/DDOS attacks** and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or destabilized. A **denial-of-service (DoS) attack** is a malicious attempt to overwhelm an online service and render it unusable.
  - **General attack detection and recovery** to **cope with IoT-specific threats**, such as compromised nodes, malicious code hacking attacks.

Contd.

- **Cyber situation awareness tools/techniques** will need to be developed to enable IoT-based infrastructures to be monitored.
- The IoT requires a **variety of access control and associated accounting schemes to support the various authorisation** and usage models that are required by users.
- **The IoT needs to handle virtually all modes of operation by itself without relying on human control**. New techniques and approaches **e.g. from machine learning, are required to lead to a self-managed IoT**.

Privacy for IoT

- As much of the information in an IoT system may be personal data, there is a requirement to **support anonymity and restrictive handling of personal information**.



Contd.

- There are a number of areas where advances are required:
  - Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties.
  - Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches.
  - Techniques to support Privacy by Design concepts, including data minimization, identification, authentication and anonymity.
  - Fine-grain and self-configuring access control mechanism emulating the real world

Contd.

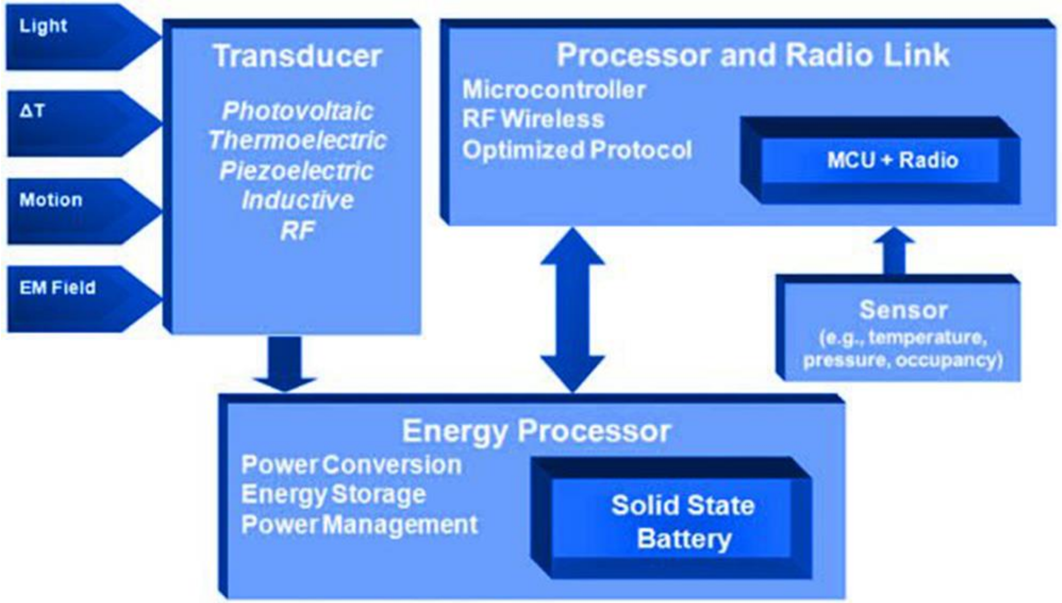
- There are a number of privacy implications arising from the ubiquity and pervasiveness of IoT devices where further research is required, including
  - **Preserving location privacy**, where location can be inferred from things associated with people.
  - **Prevention of personal information** inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.
  - **Keeping information as local as possible** using decentralised computing and key management.
  - Use of soft Identities, where the real identity of the user can be used to generate various soft identities for specific applications. Each soft identity can be designed for a specific context or application without revealing unnecessary information, which can lead to privacy breaches.

Energy Harvesting

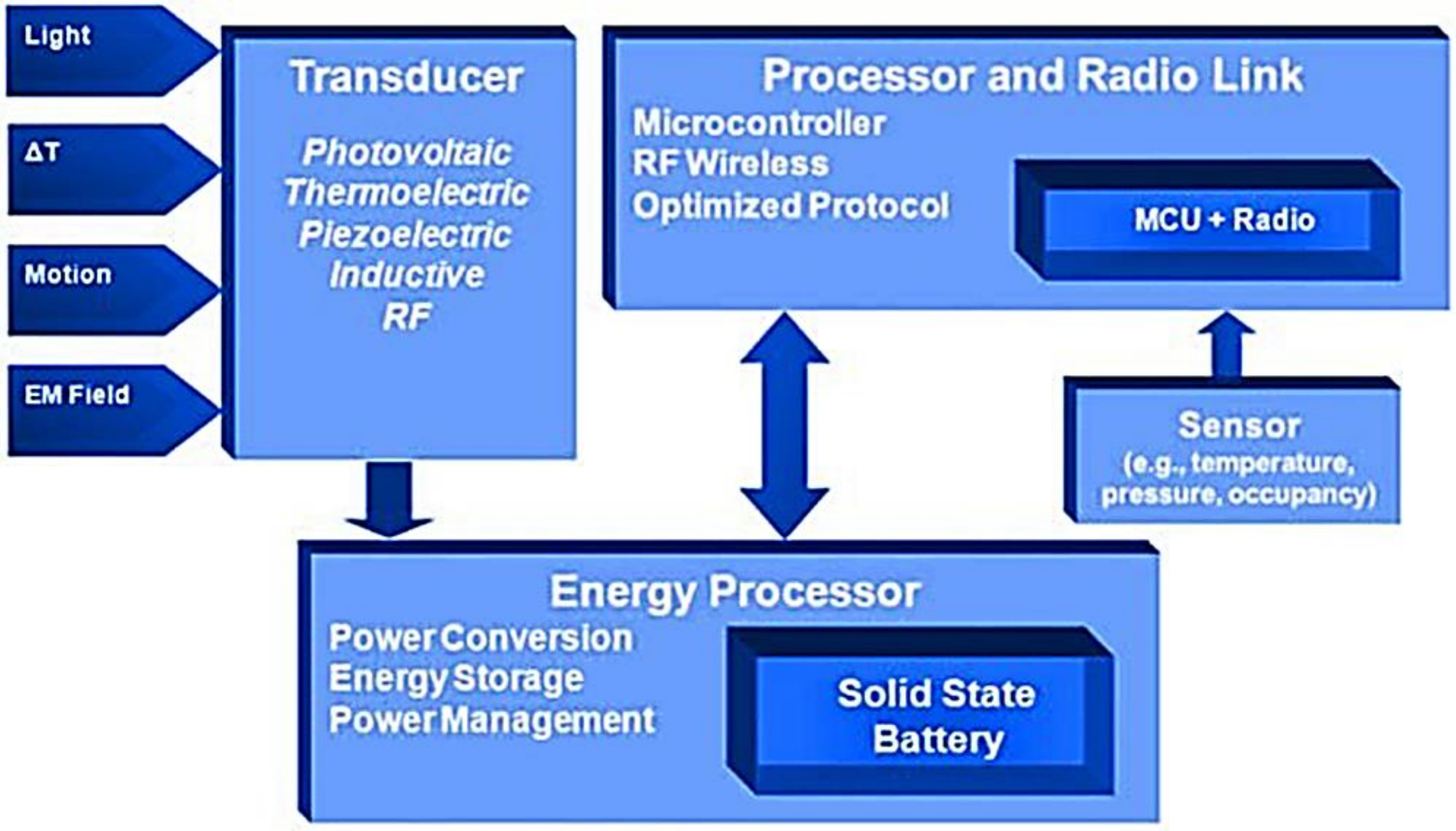
- Four main ambient energy sources are present in our environment: mechanical energy, thermal energy, radiant energy and chemical energy.
- The power consumption varies depending on the communication protocols and data rate used to transmit the date.
- The approximate power consumption for different protocols is as following 3G-384kbps-2W, GPRS-24kbps-1W, WiFi-10Mbps-32–200mW, Bluetooth-1Mbps-2.5–100 mW, and Zigbee-250kbps-1mW.
- Ambient light, thermal gradients, vibration/motion or electromagnetic radiation can be harvested to power electronic devices.

Energy Harvesting … Contd.

- The major components of an autonomous wireless sensor are the energy harvesting transducer, energy processing, sensor, microcontroller and the wireless radio.
- For successful energy harvesting implementations there are three key areas in the energy processing stage that must be addressed: energy conversion, energy storage, and power management.



[Energy harvesting - components of an autonomous wireless sensor]



[Energy harvesting - components of an autonomous wireless sensor]

Energy Harvesting … Contd.

- The development of energy harvesting and storage devices is instrumental to the realization of the ubiquitous connectivity that the IoT proclaims.
- The energy harvesting wireless sensor solution is able to generate a signal from an extremely small amount of energy.
- **From just 50 µWs a standard energy harvesting wireless module can easily transmit a signal 300 meters**