CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

University Institute of Engineering

AIT-CSE (IoT)

Course Name- Privacy and Security in IoT

Course Code- CSD- 433

UNIT 1-INTRODUCTION: SECURING THE INTERNET OF THINGS

Topic – Requirement of security in IoT architecture

Lecture – 1.1

Presented by

Er. Gaurav Soni (E9610)

Assistant Professor, AIT-CSE

Privacy and Security in IoT

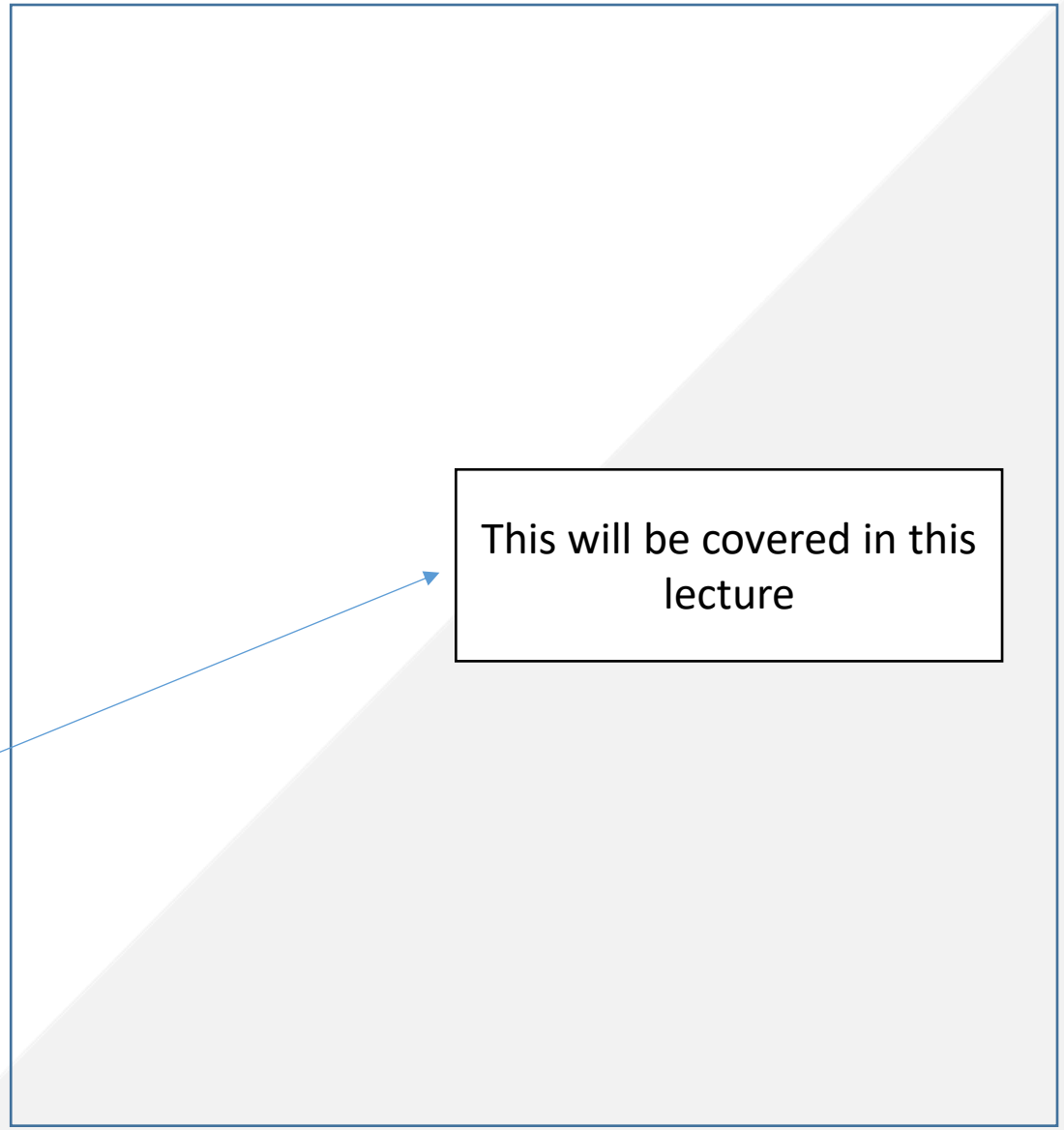
Course Objectives

CO Number	Title
CO1	To identify various privacy and security requirements in Internet of Things
CO2	To learn cryptographic techniques for a secure IoT system
CO3	To understand various Trust Models used in IoT

Privacy and Security in IoT

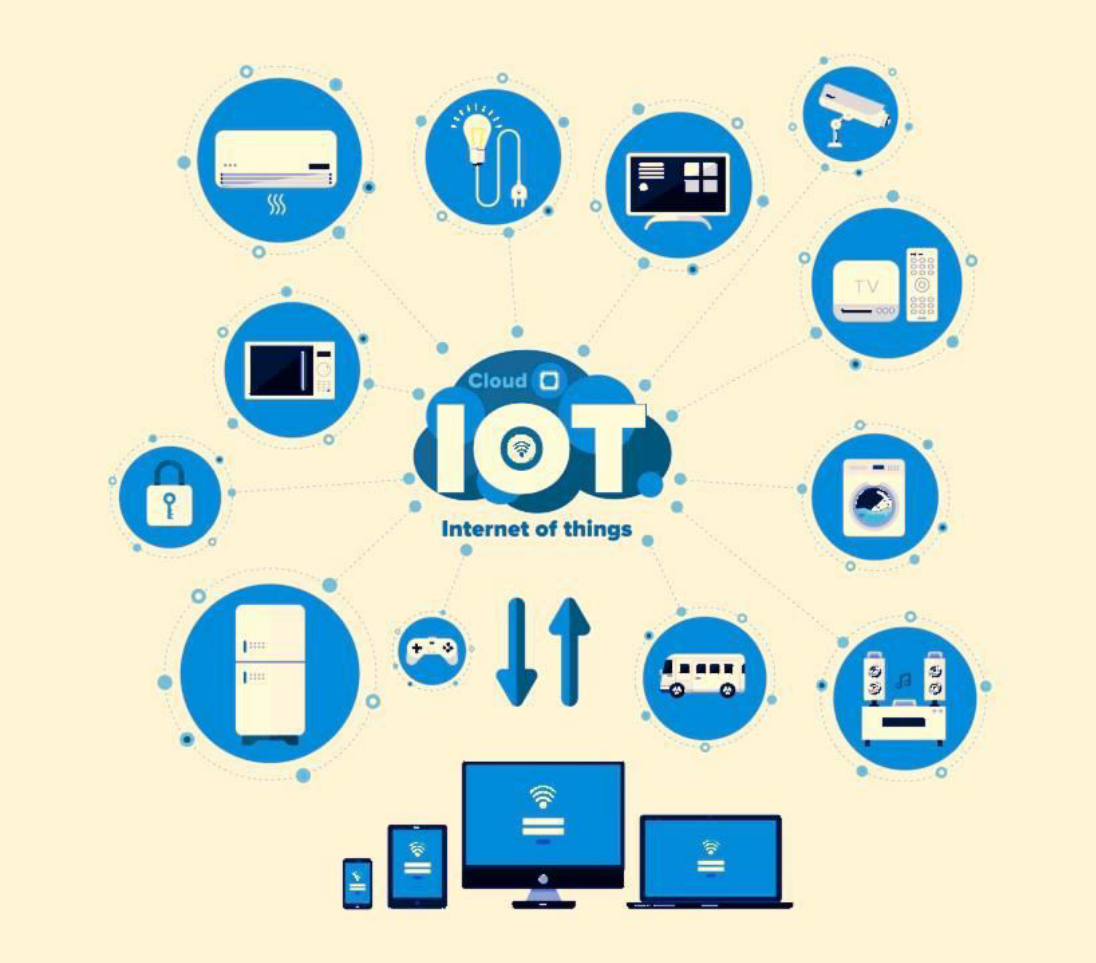
Course Outcome

CO Number	Title	Level
CO1	After successful completion of this course students will be able to understand the security requirements in IoT.	**Understand**
CO2	After successful completion of this course students will be able to understand the authentication credentials and access control.	**Understand**
CO3	After successful completion of this course students will be able to implement security algorithms to make a secure IoT system.	Implement



What is IoT ?

The Internet of Things (**IoT**) describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.



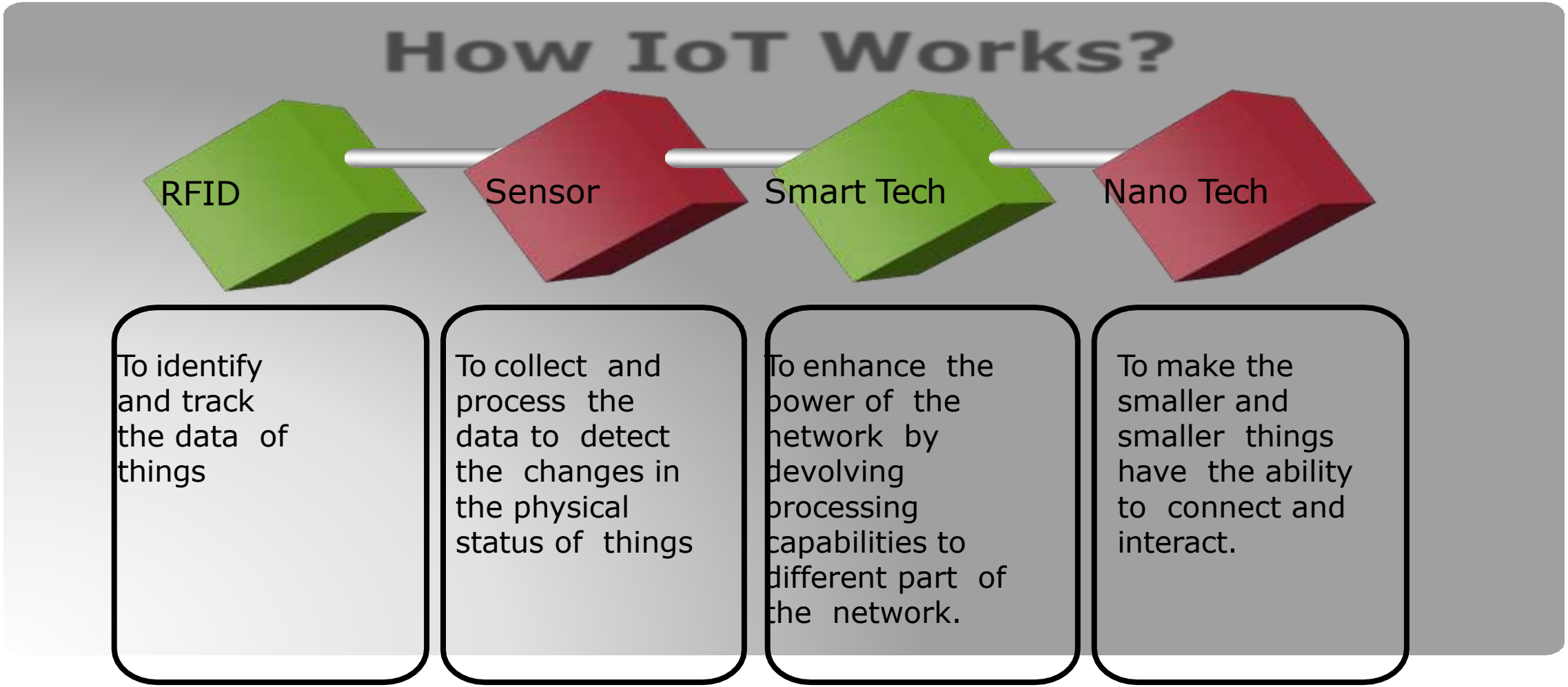
How IoT Works?

Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world.

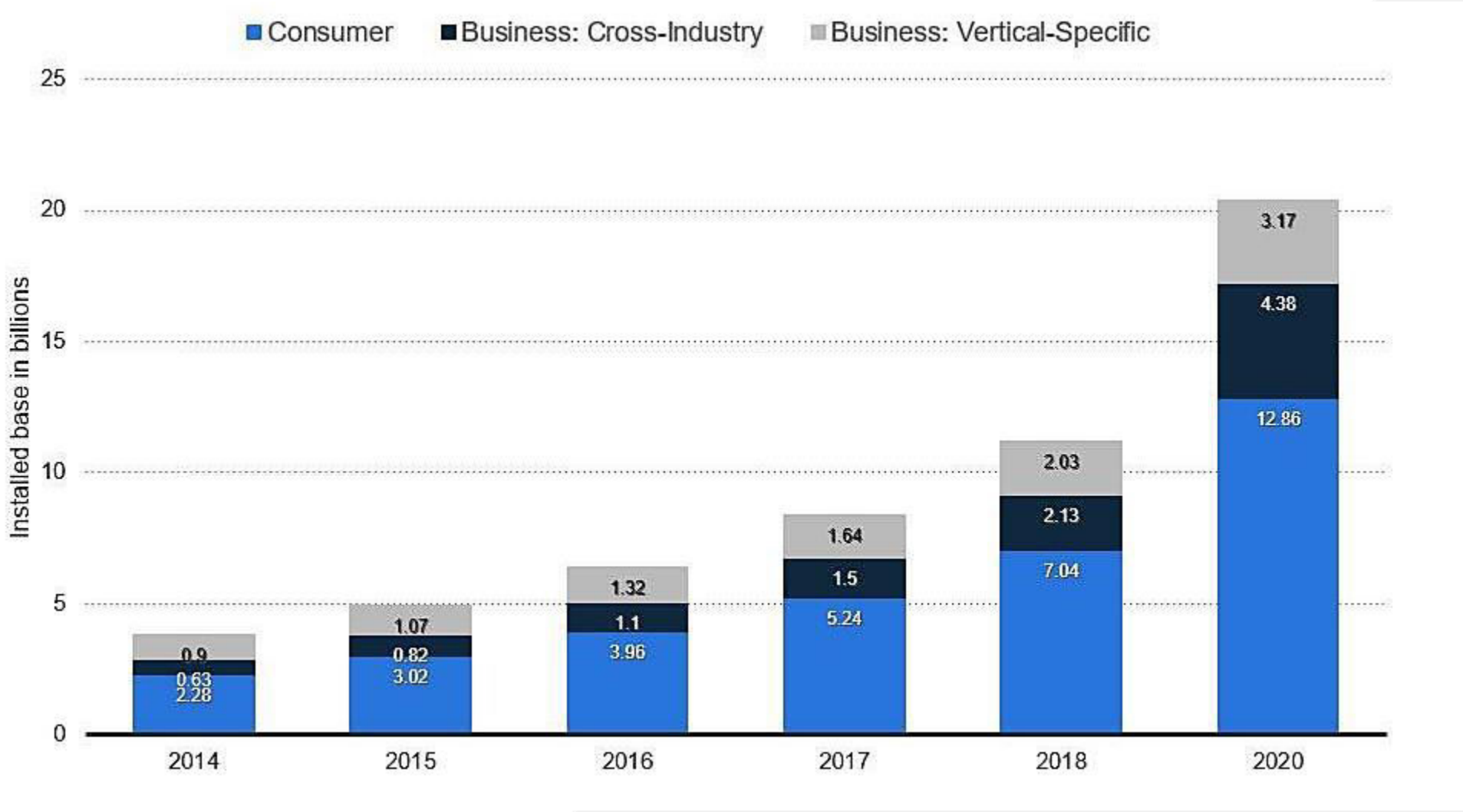
These capabilities include:

- ***Communication and cooperation***
- ***Addressability***
- ***Identification***
- ***Sensing***
- ***Actuation***
- ***Embedded information processing***
- ***Localization***
- ***User interfaces***

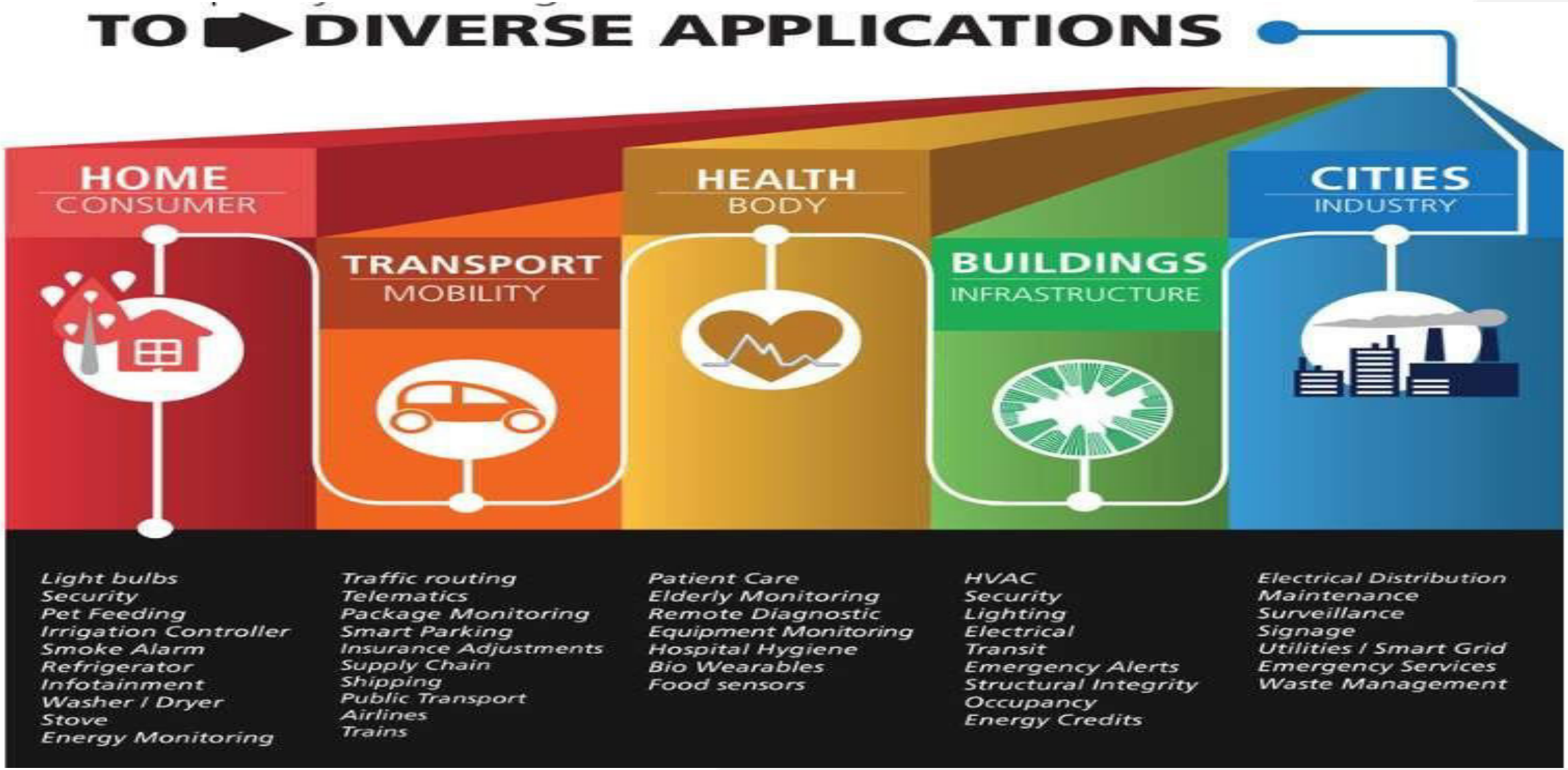
How IoT Works?



IoT Growth Graph



IoT Applications



What are Privacy and Security Issues?

Privacy and Security issues are major barrier in the adoption of IoT system at mass level

Privacy Issues vs. Security Issues

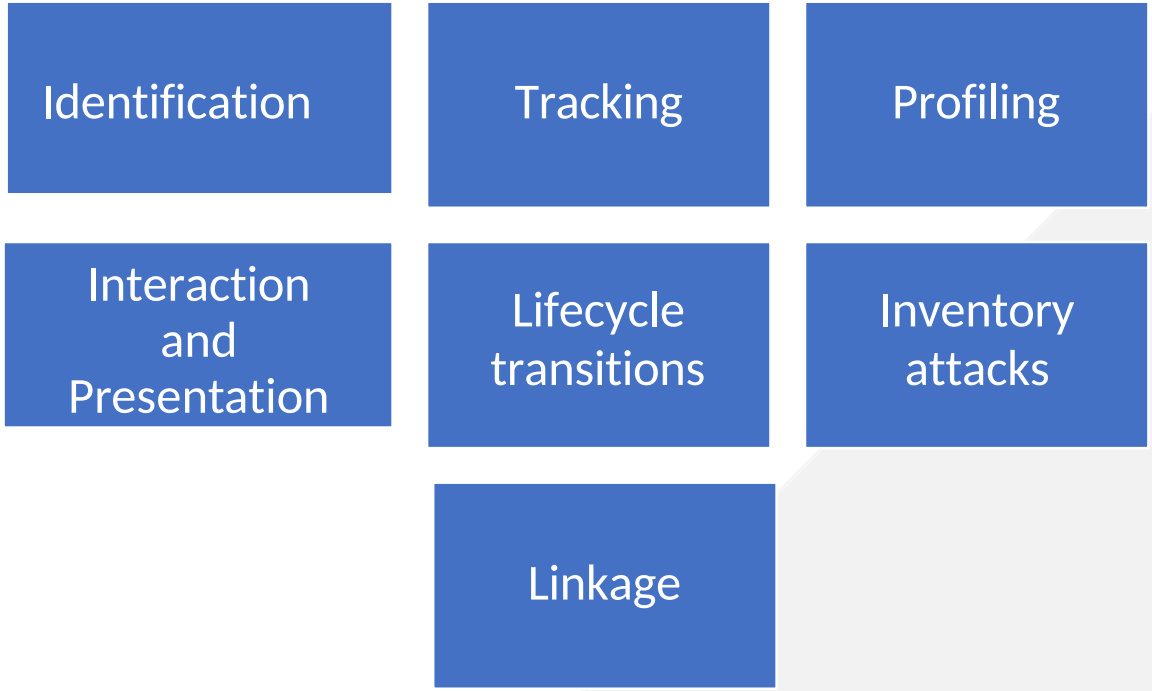
Security Issues?

Security issues are more concern about hacking of smart devices.

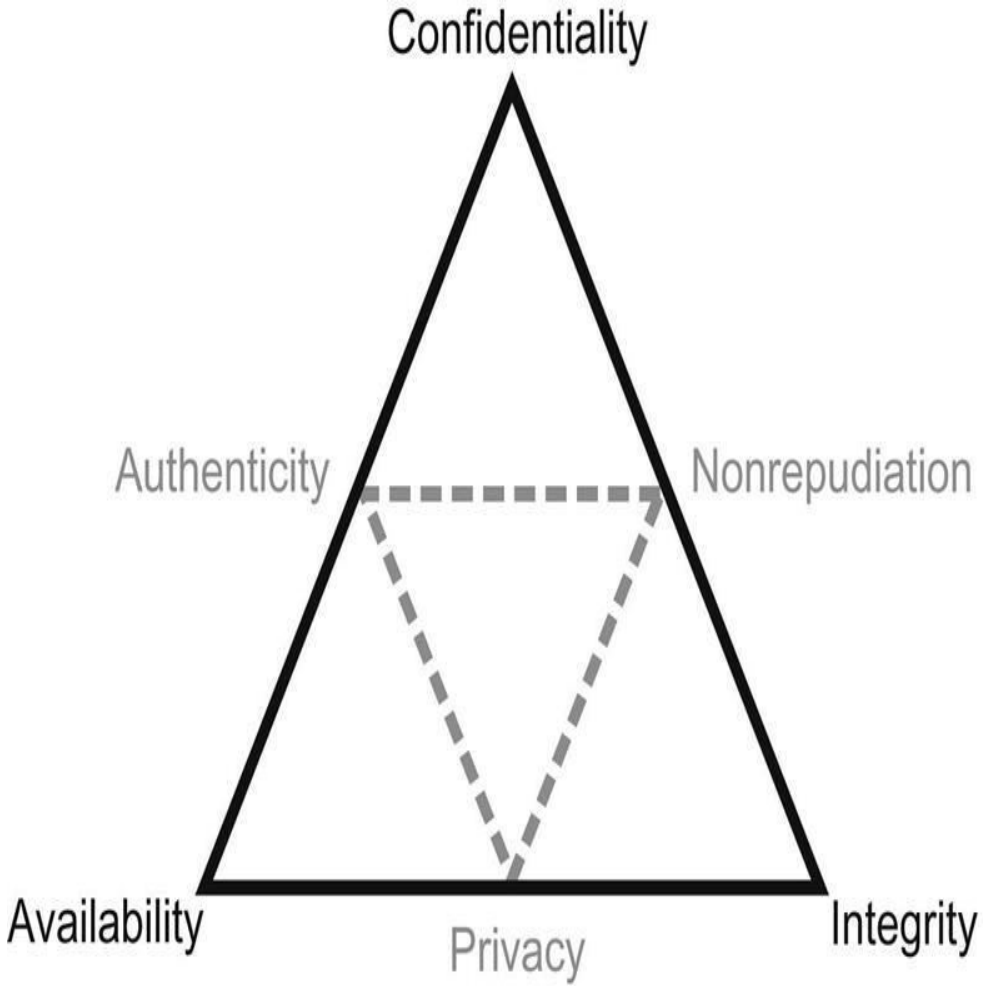
Privacy Issues?

Risk of leakage of personal data of any person is associated with privacy issues in IoT.

7 Threats to Privacy in the IoT



SECURITY REQUIREMENTS IN IoT



- **Confidentiality**—data is secured to authorized parties
- **Integrity**—data is trusted
- **Availability**—data is accessible when and where needed
- **Nonrepudiation**—service provides a trusted audit trail
- **Authenticity**—components can prove their identity
- **Privacy**—service does not automatically see customer data

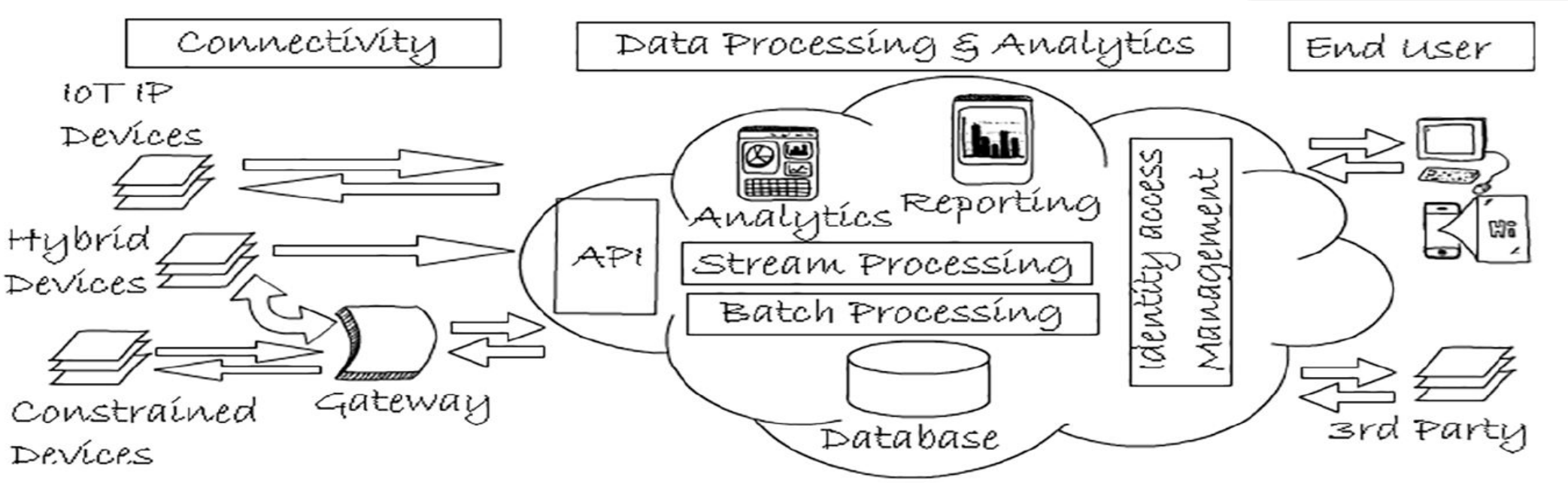
TECHNOLOGICAL CHALLENGES OF IoT

At present IoT is faced with many challenges, such as:

- Scalability
- Technological Standardization
- Inter operability
- Discovery
- Software complexity
- Data volumes and interpretation
- Power Supply
- Interaction and short range communication
- Wireless communication
- Fault tolerance

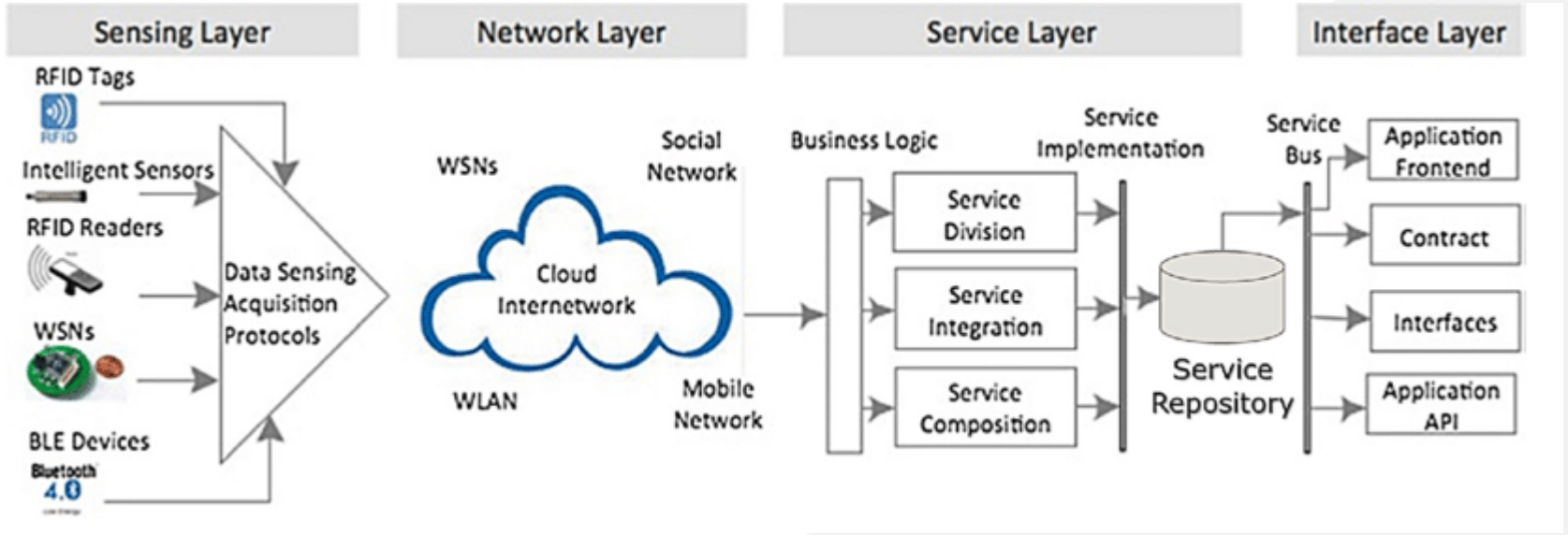
Four Layer Security Architecture & Its Requirement

By this security architecture we able to understand treats at various levels of IoT functioning



Four Layer Security Architecture & Its Requirement

By this security architecture we able to understand treats at various levels of IoT functioning



IoT - The security challenge

- Devices are not reachable
  - Most of the time a device is not connected
- Devices can be lost and stolen
  - Makes security difficult when the device is not connected
- Devices are not crypto-engines
  - Strong security difficult without processing power
- Devices have finite life
  - Credentials need to be tied to lifetime
- Devices are transportable
  - Will cross borders
- Devices need to be recognised by many readers
  - What data is released to what reader?

Security Architecture & Its Requirement

Sensing/Perception layer - Collect the information using various sensors.

Possible attacks on this level are :

- Eavesdropping
- Node Capture
- Fake Node

Security Architecture & Its Requirement

Sensing/Perception layer

In this layer, the security concerns can be classified into two main categories:

- The security requirements at IoT end-node: physically security protection, access control, authentication, nonrepudiation, confidentiality, integrity, availability, and privacy.
- The security requirements in sensing layer: confidentiality, data source authentication, device authentication, integrity, availability, and timeless.

Security Architecture & Its Requirement

Network Layer - It carries and transmits the information collected from the physical objects through sensors.

Possible types attacks are:

- Denial of Service (DoS) Attack
- Main-in-The-Middle (MiTM) Attack

Security Architecture & Its Requirement

Network Layer – The security requirements in network layer involve

- Overall security requirements, including confidentiality, integrity, privacy protection, authentication, group authentication, keys protection, availability, etc.
- Privacy leakage: Since some IoT devices physically located in untrusted places, which cause potential risks for attackers to physically find the privacy information such as user identification, etc.
- Communication security: It involves the integrity and confidentiality of signaling in IoT communications.

Security Architecture & Its Requirement

Application Layer - Application layer defines all applications that use the IoT technology

Common security threats and problem of application layer are:

- Cross Site Scripting
- Malicious Code Attack

Security Architecture & Its Requirement

Application Layer - For the application maintenance, following security requirements will be involved:

- Remote safe configuration, software downloading and updating, security patches, administrator authentication, unified security platform, etc.
- For the security requirements on communications between layers:
- Integrity and confidentiality for transmission between layers, cross-layer authentication and authorization, sensitive information isolation, etc.

Security Architecture & Its Requirement

Security of IoT architecture may improved by introducing additional layer

Support Layer –

- In four-layer architecture, information is sent to a support layer that is obtained from a perception layer.
- The support layer has two responsibilities. It confirms that information is sent by the authentic users and protected from threats.

References

1. Li Da Xu, Securing Internet of Things, Algorithms, and Implementations, Elsevier
2. Muhammad Burhan, “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey” Sensors, MDPI

Study Link : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453/#:~:text=Security%20and%20privacy%20are%20the,the%20confidential%20information%20of%20objects.

Home Assignment

1. Explore various protocols used in IoT network.
2. What is the purpose of fourth layer used in IoT security architecture , i.e Support Layer

THANK YOU

For queries
Email: gaurav.e9610@cumail.in