CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

University Institute of Engineering

AIT-CSE

Privacy and Security in IoT - CSD- 433

Topic – Security Architecture in the Internet of Things

Lecture – 1.5

Delivered by

Er. Gaurav Soni (E9610)

Assistant Professor, AIT-CSE

Privacy and Security in IoT

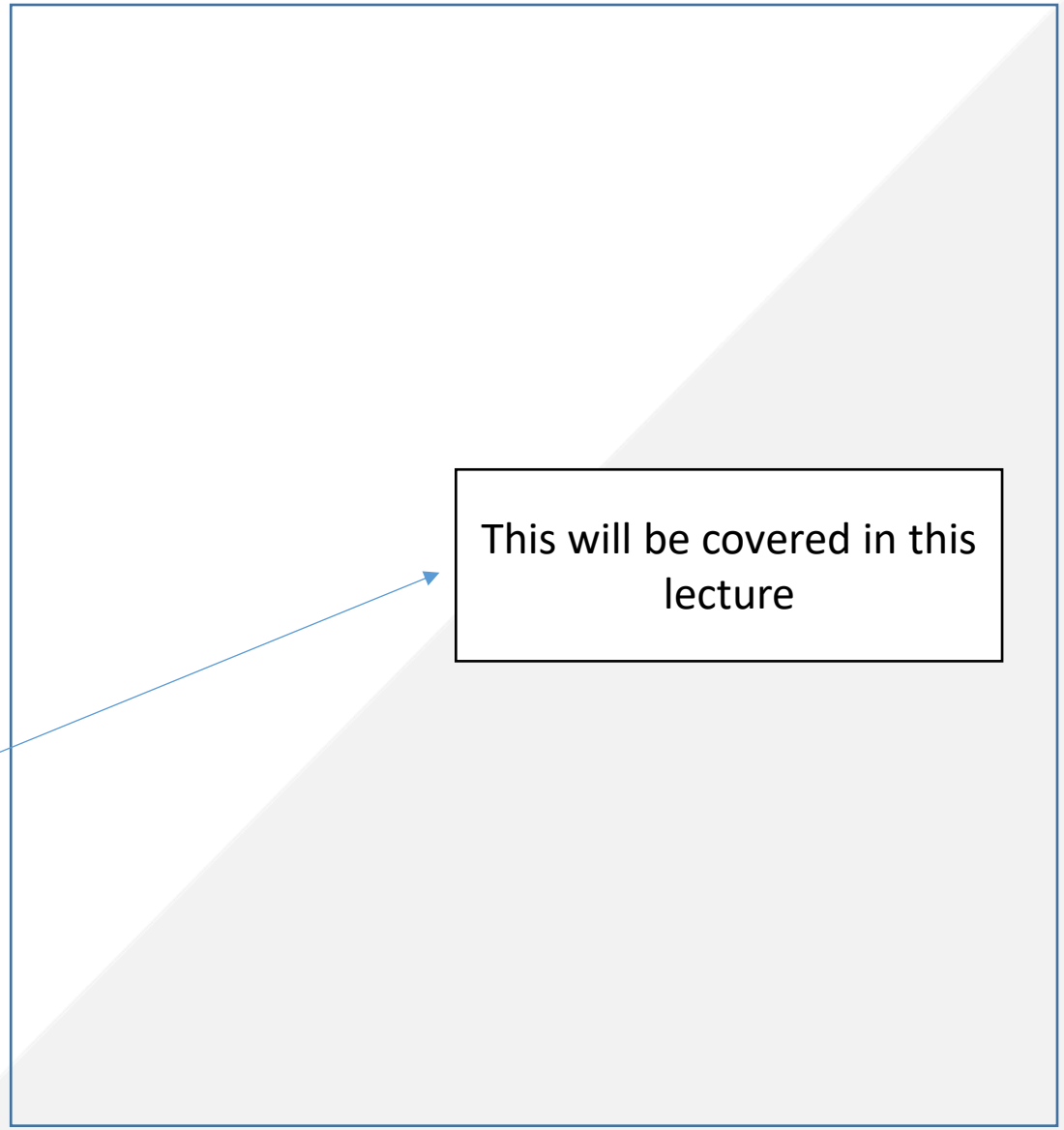
Course Objectives

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

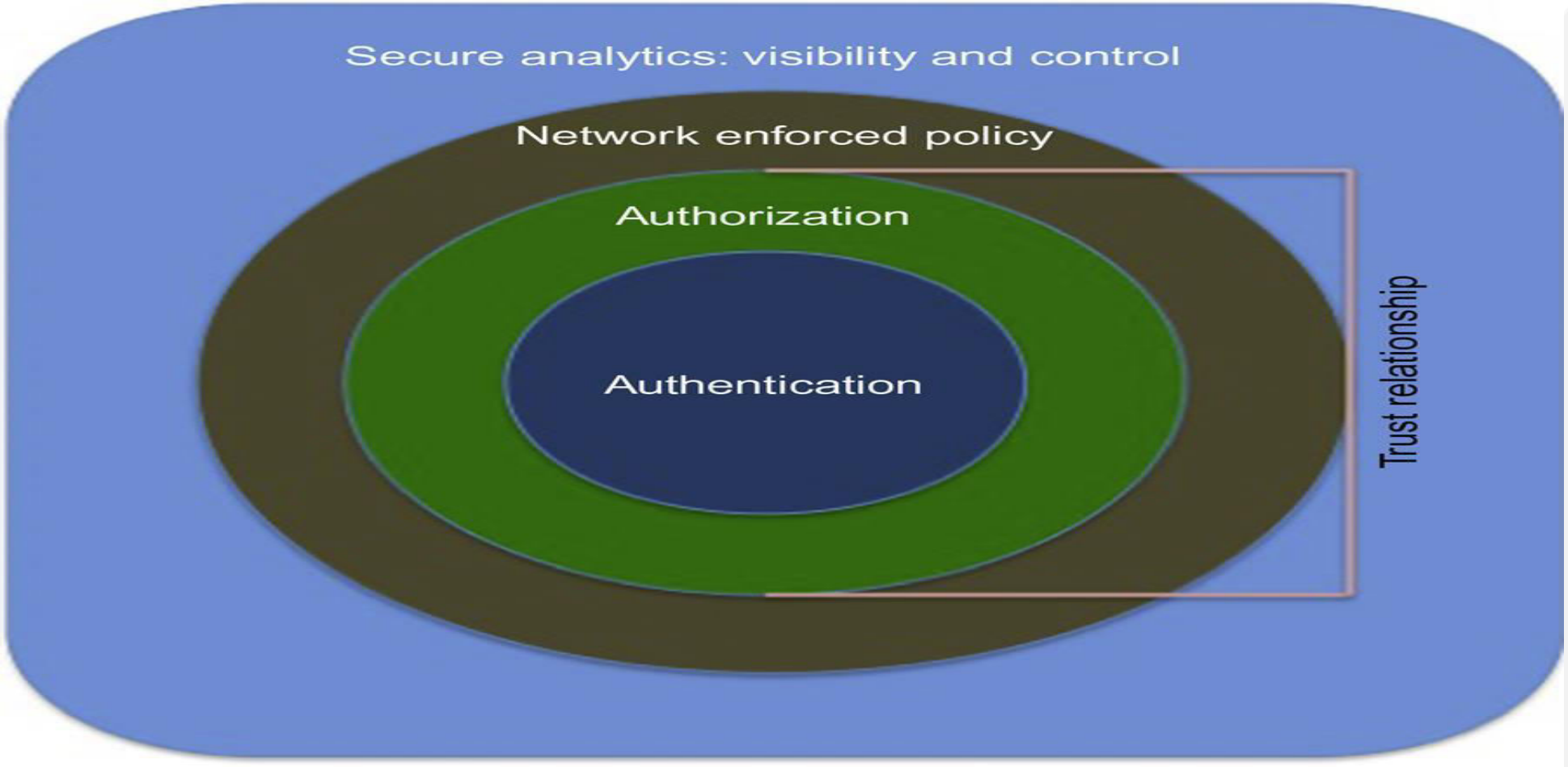
Privacy and Security in IoT

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



SECURITY in IoT

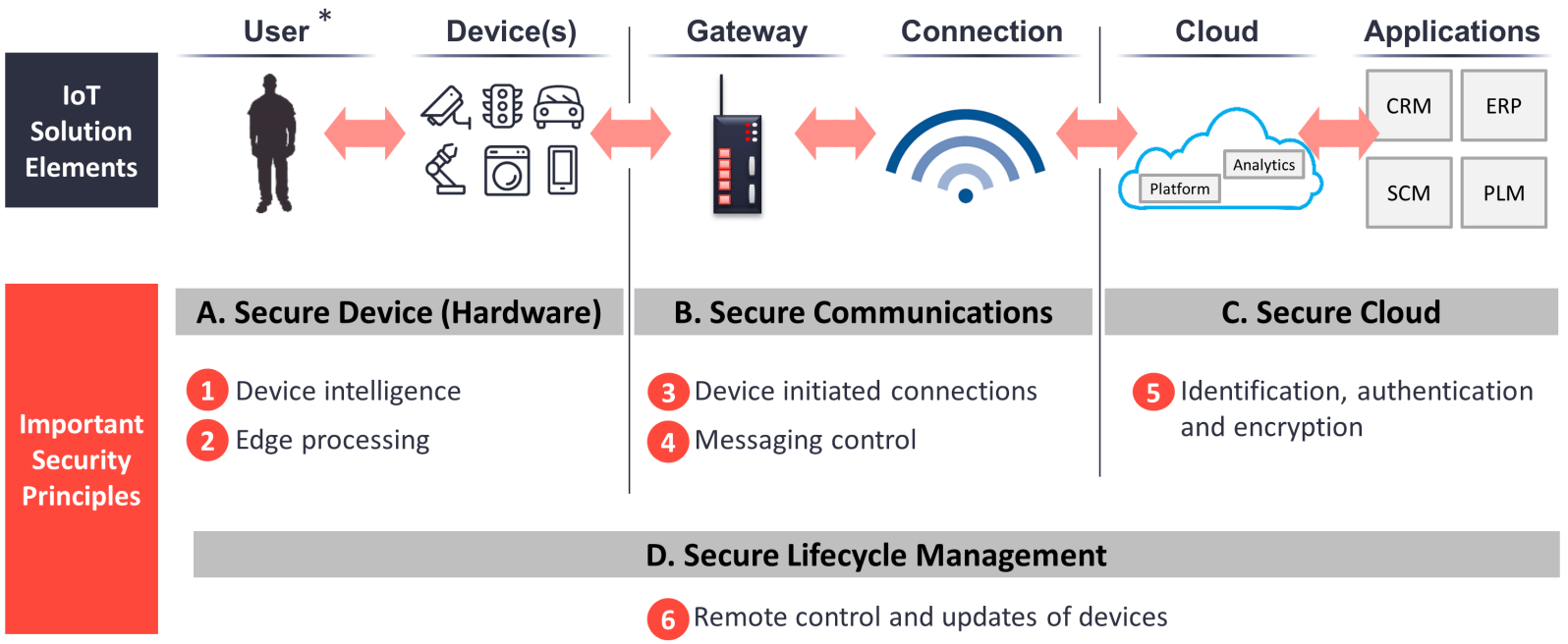


Top 10 Vulnerabilities in IoT

Security Concerns	Interface Layer	Service Layer	Network Layer	Sensing Layer
Insecure web interface	√	√	√	
Insufficient authentication/authorization	√	√	√	√
Insecure network services		√	√	
Lack of transport encryption		√	√	
Privacy concerns		√	√	√
Insecure cloud interface	√			
Insecure mobile interface	√		√	√
Insecure security configuration	√	√	√	
Insecure software/firmware	√		√	
Poor physical security			√	√

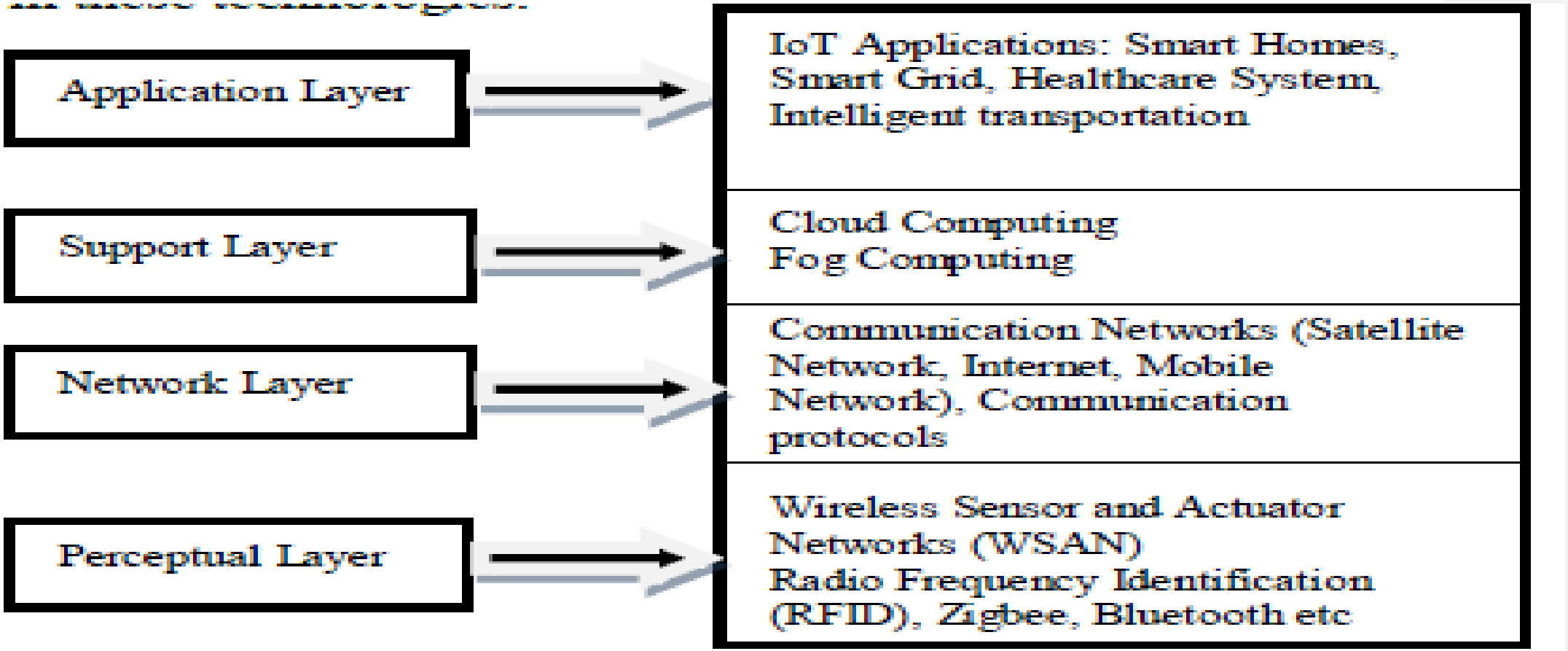
IoT security Principles

Six principles of IoT Cyber Security across the stack

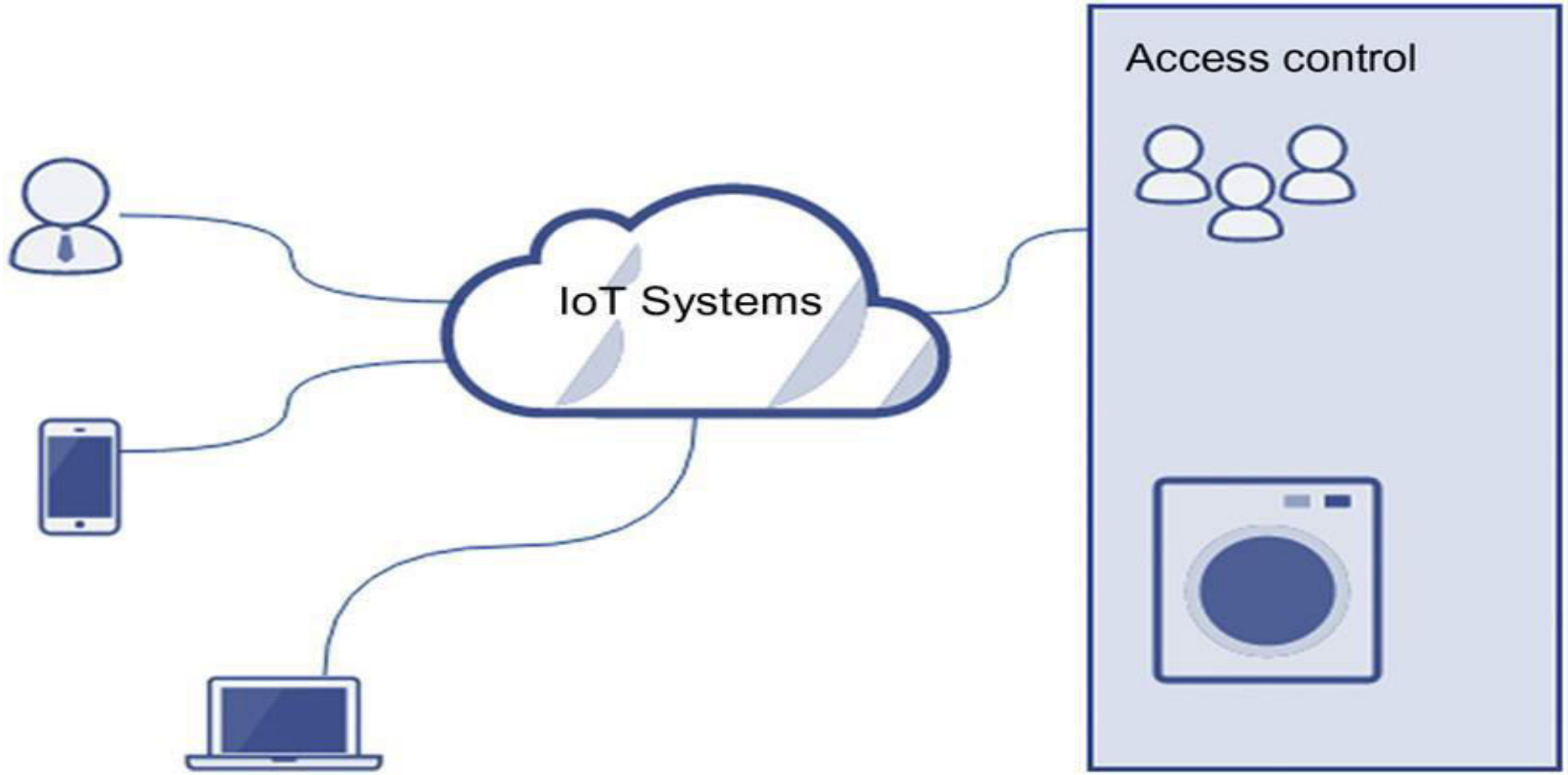


ght © 2016 by www.iot-analytics.com All rights reserved

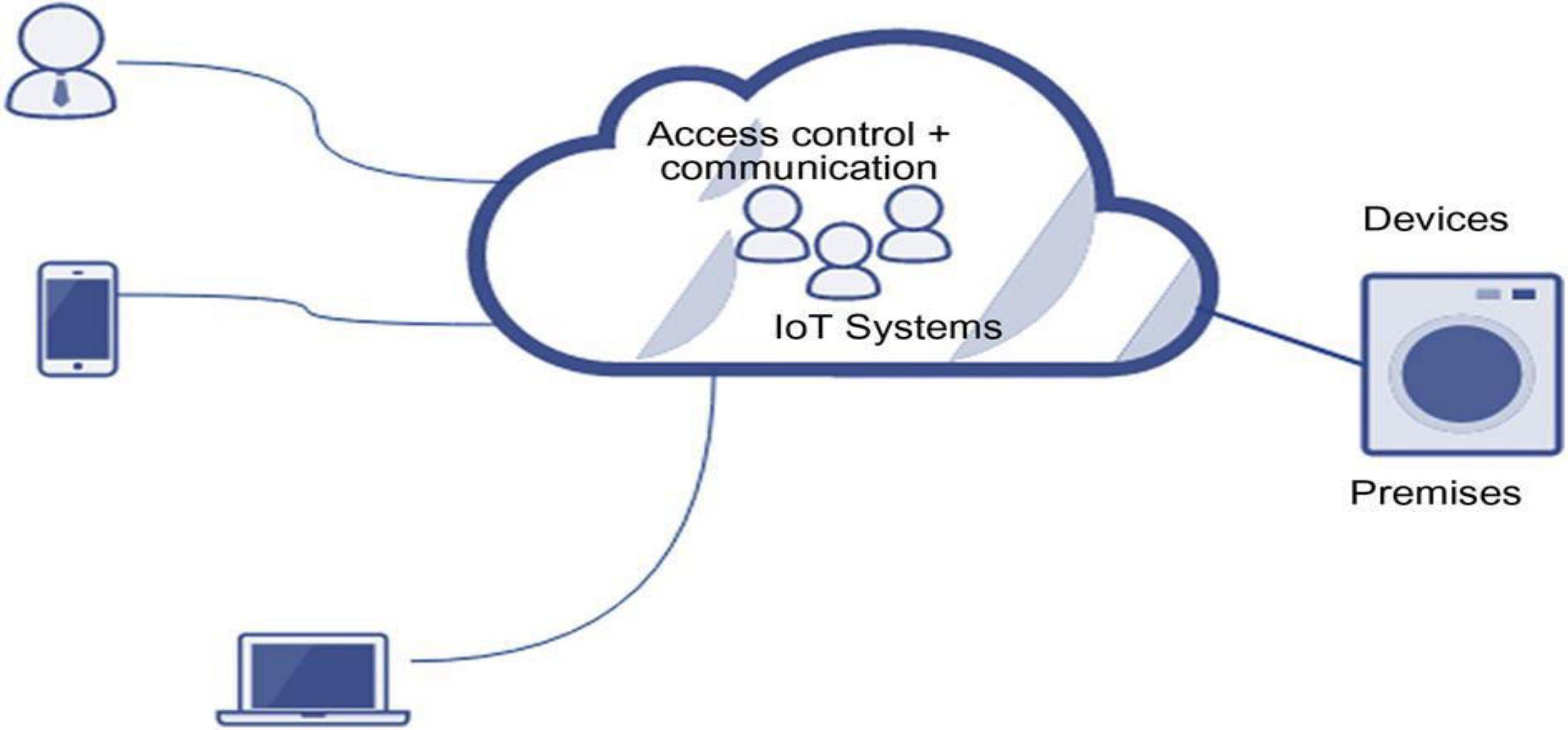
IoT Security architecture



ACCESS CONTROL LIST-BASED SYSTEMS



CAPABILITY-BASED ACCESS



Building Security for IoT

Security must be addressed throughout the device lifecycle, from initial design to the operational environment

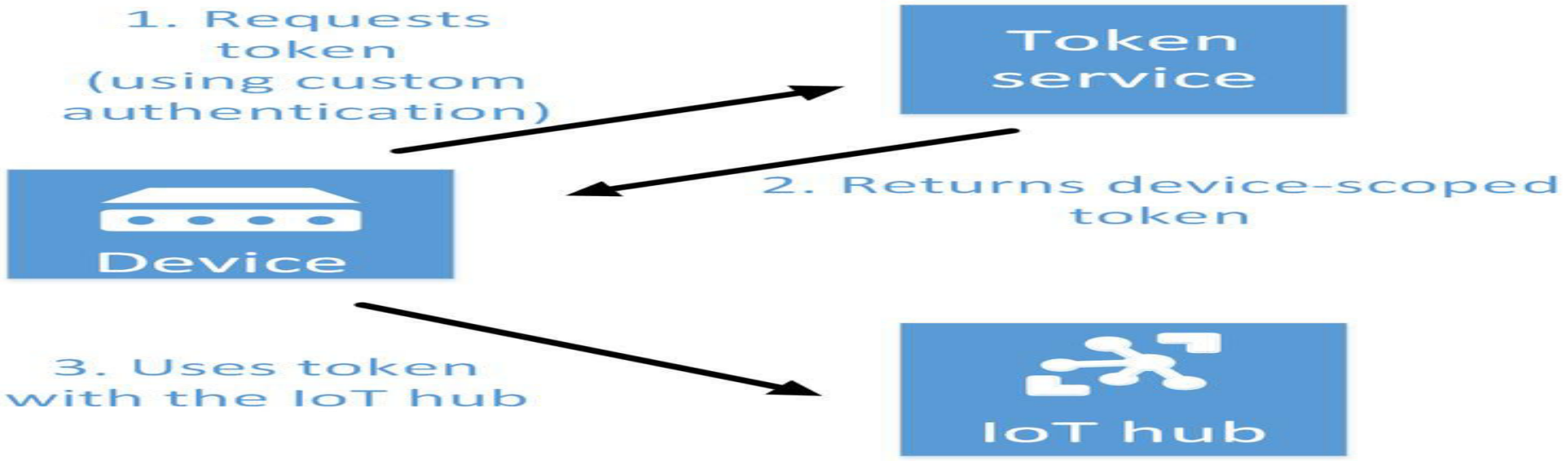
1. Secure booting
2. Access control
3. Device authentication
4. Firewalling and IPS

Secure Booting

- When power is first introduced to the device, the authenticity and integrity of the software on the device is **verified using cryptographically generated digital signature.**
- A digital signature attached to the software image and verified by the device ensures that only the software that has been authorized to **run on that device**, and signed by the entity that authorized it , will be loaded

Device authentication

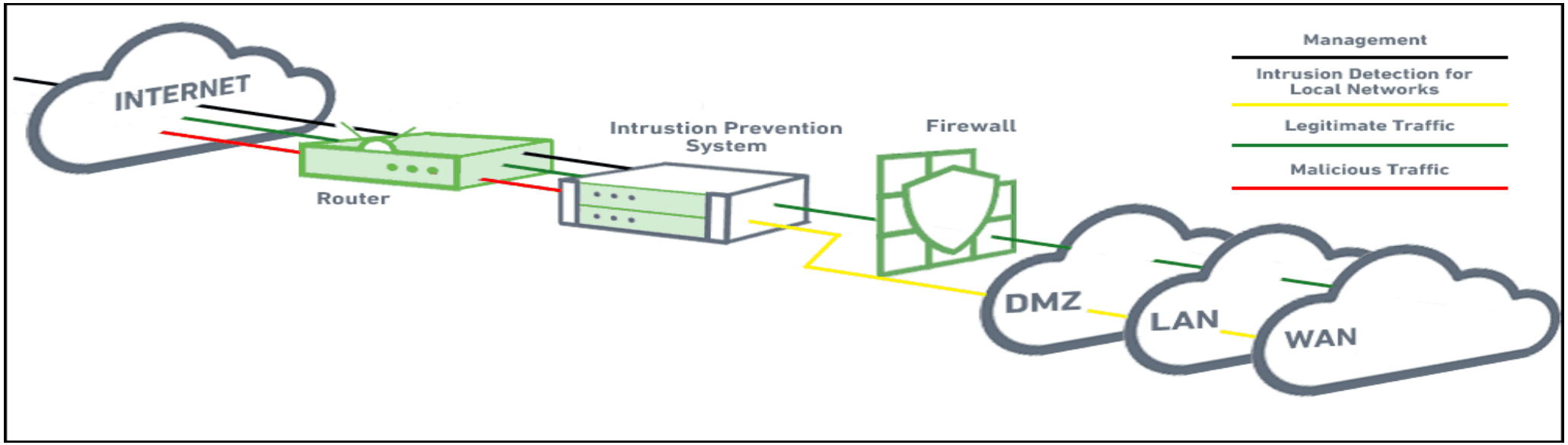
- When a device is **plugged** into network, it should **authenticate** itself prior receiving or transmitting data.



Firewalling and IPS

- The device needs a **firewall** or **deep packet**
- **inspection capability** to control traffic that

is **destined to terminate at the devices**.



Updates and patches

Once the device is in operation, it will start receiving **hot patches** and **software updates**. software updates security patches must be delivered in such a way that conserves the **limited bandwidth** and internet connectivity of an embedded device.

References

1. Li Da Xu, Securing Internet of Things, Algorithms, and Implementations, Elsevier

Home Assignment

1. Name some security threats held at network Layer.

THANK YOU

For queries
Email: gaurav.e9610@cumail.in