CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

University Institute of Engineering

AIT-CSE

Privacy and Security in IoT - CSD- 433

Topic – Security Requirements in IoT Architecture and types of security attack

Lecture – 1.2

Delivered by

Er. Gaurav Soni (E9610)

Assistant Professor, AIT-CSE

Privacy and Security in IoT

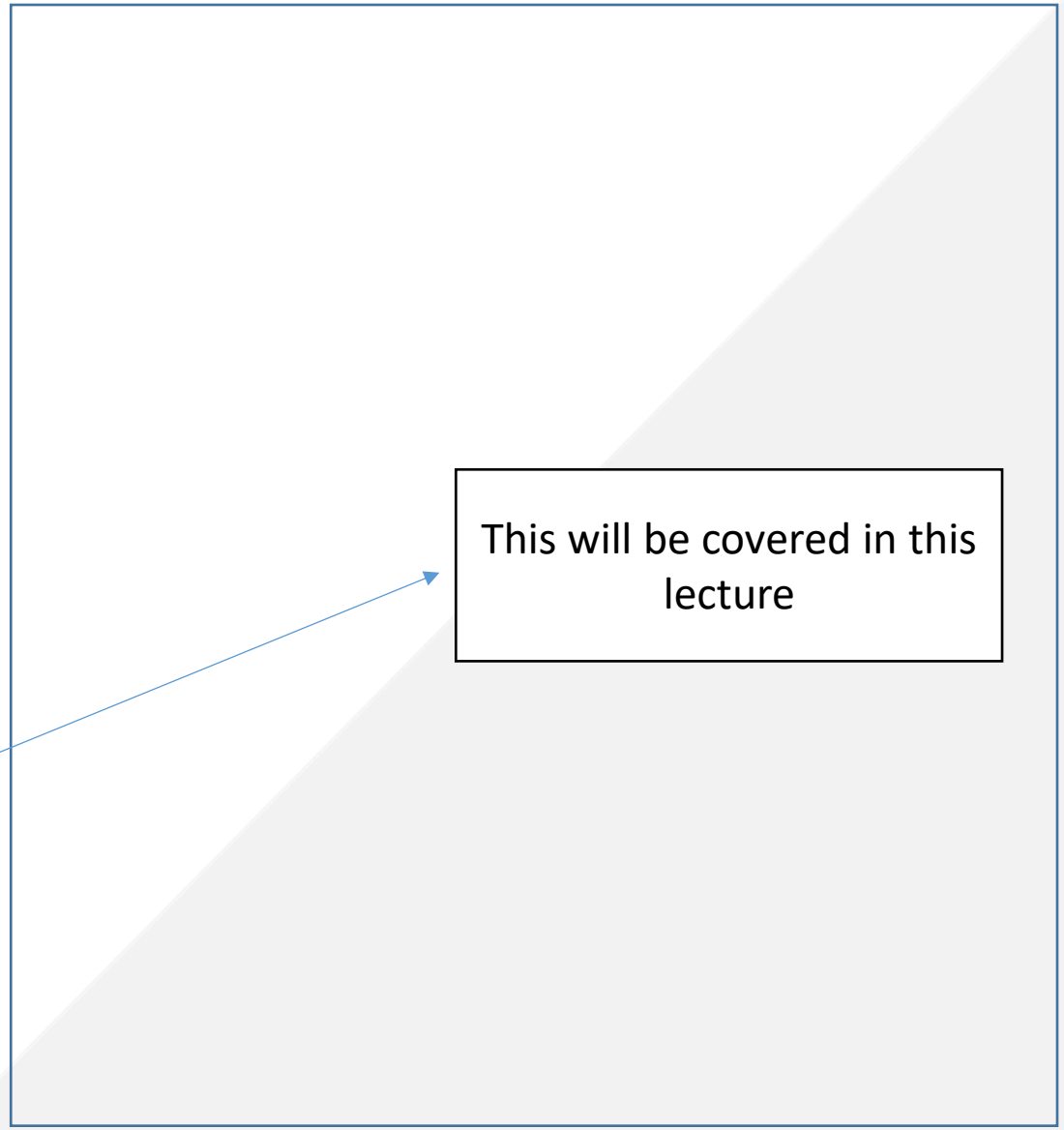
Course Objectives

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

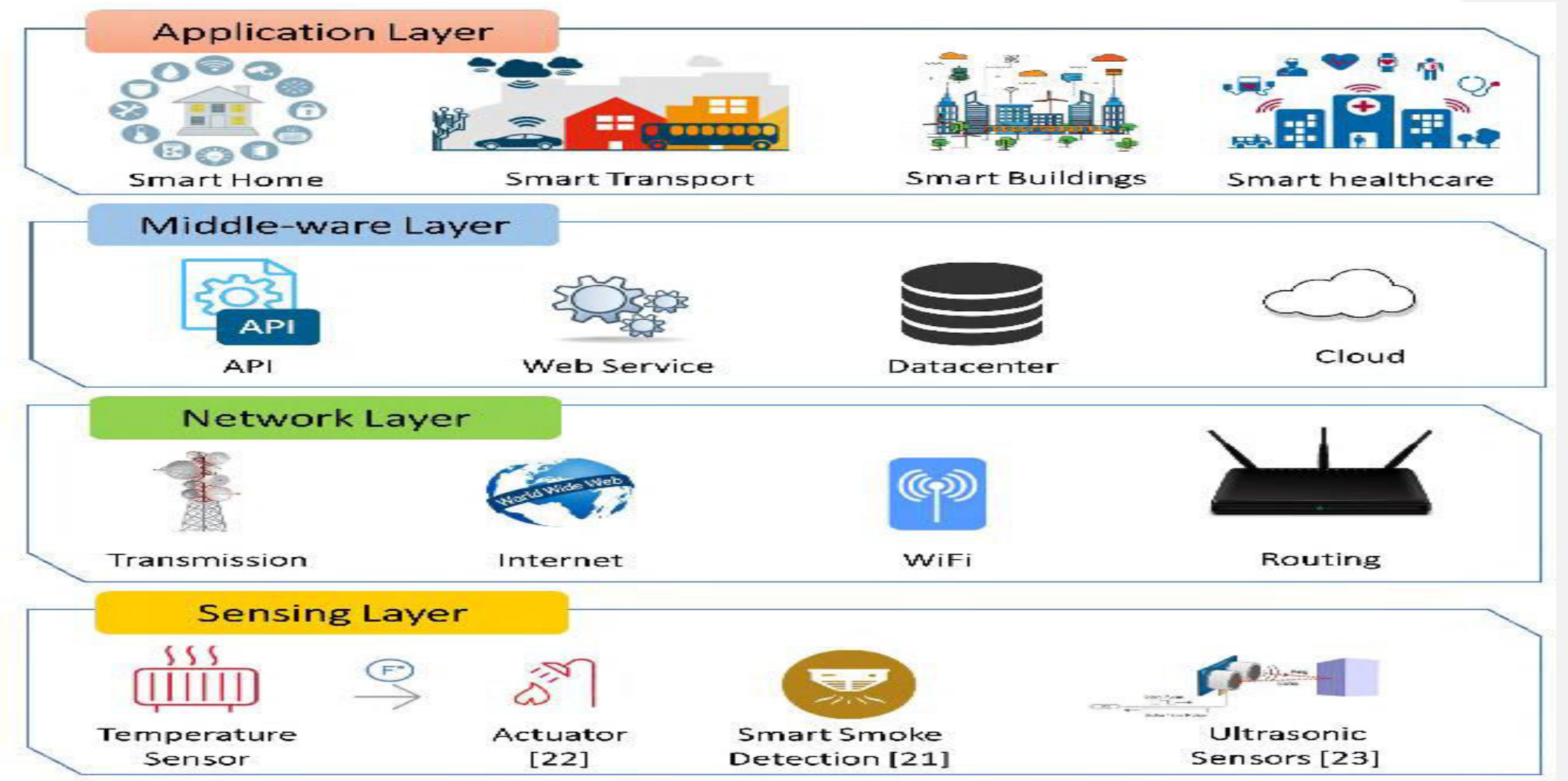
Privacy and Security in IoT

Course Outcome

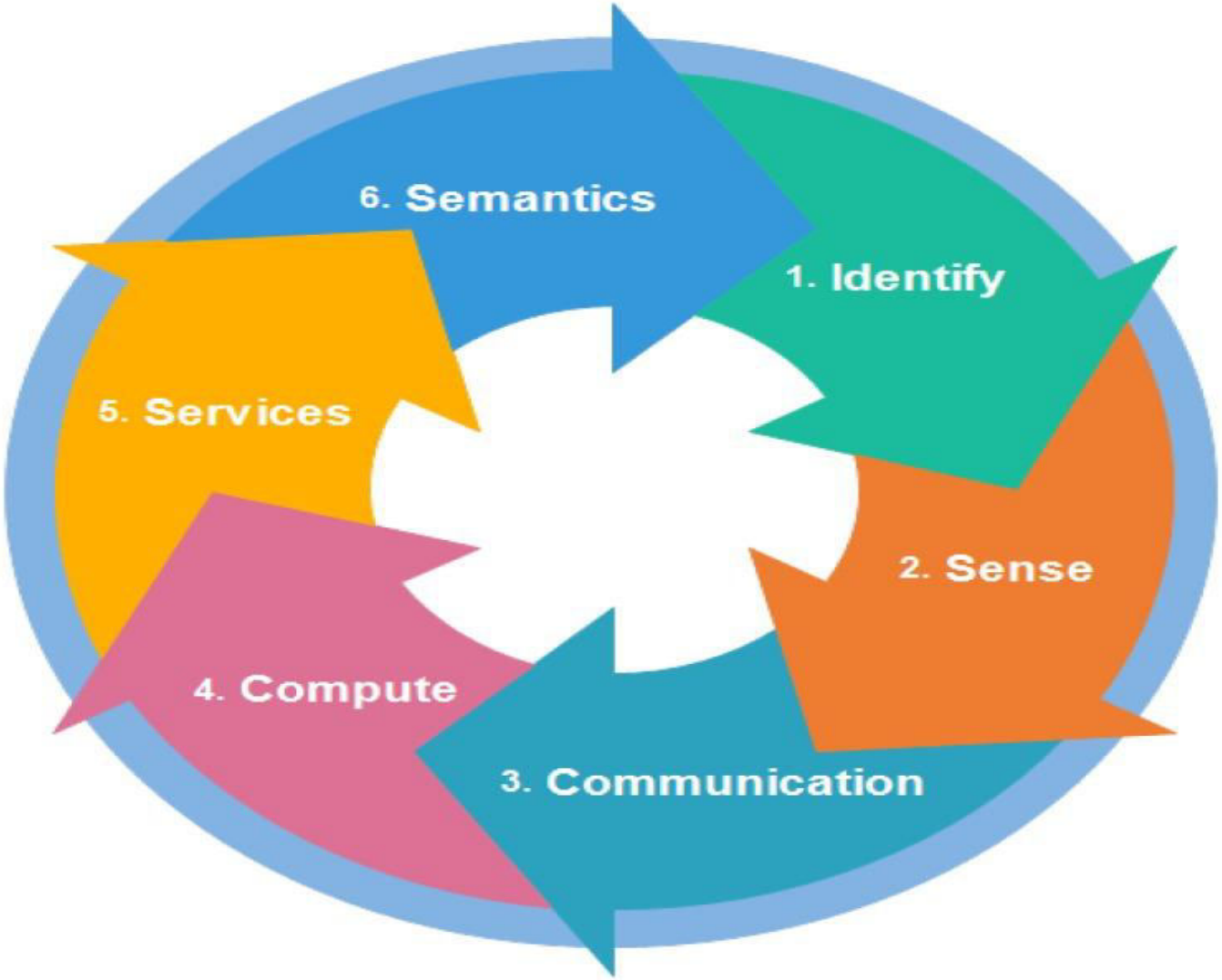
CO Number	Title	Level
CO1	After successful completion of this course students will be able to understand the security requirements in IoT.	**Understand**
CO2	After successful completion of this course students will be able to understand the authentication credentials and access control.	**Understand**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



IoT System Architecture



The IoT elements



Application Layer

- Large users accessibility
- Some critical applications
- Tested security methods

Transportation Layer

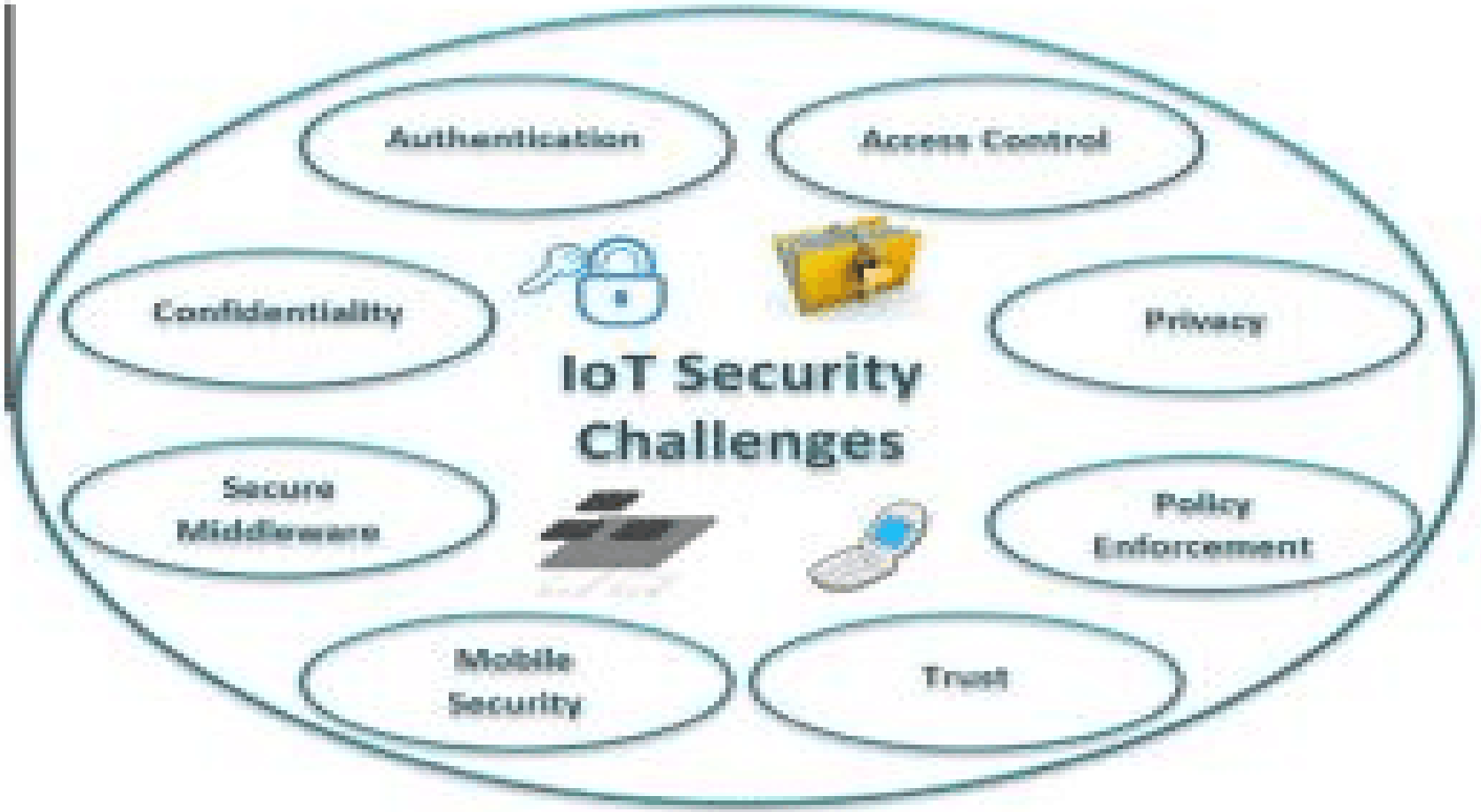
- Heterogeneous networks
- Intensive research about vulnerabilities

Perception Layer

High Risk

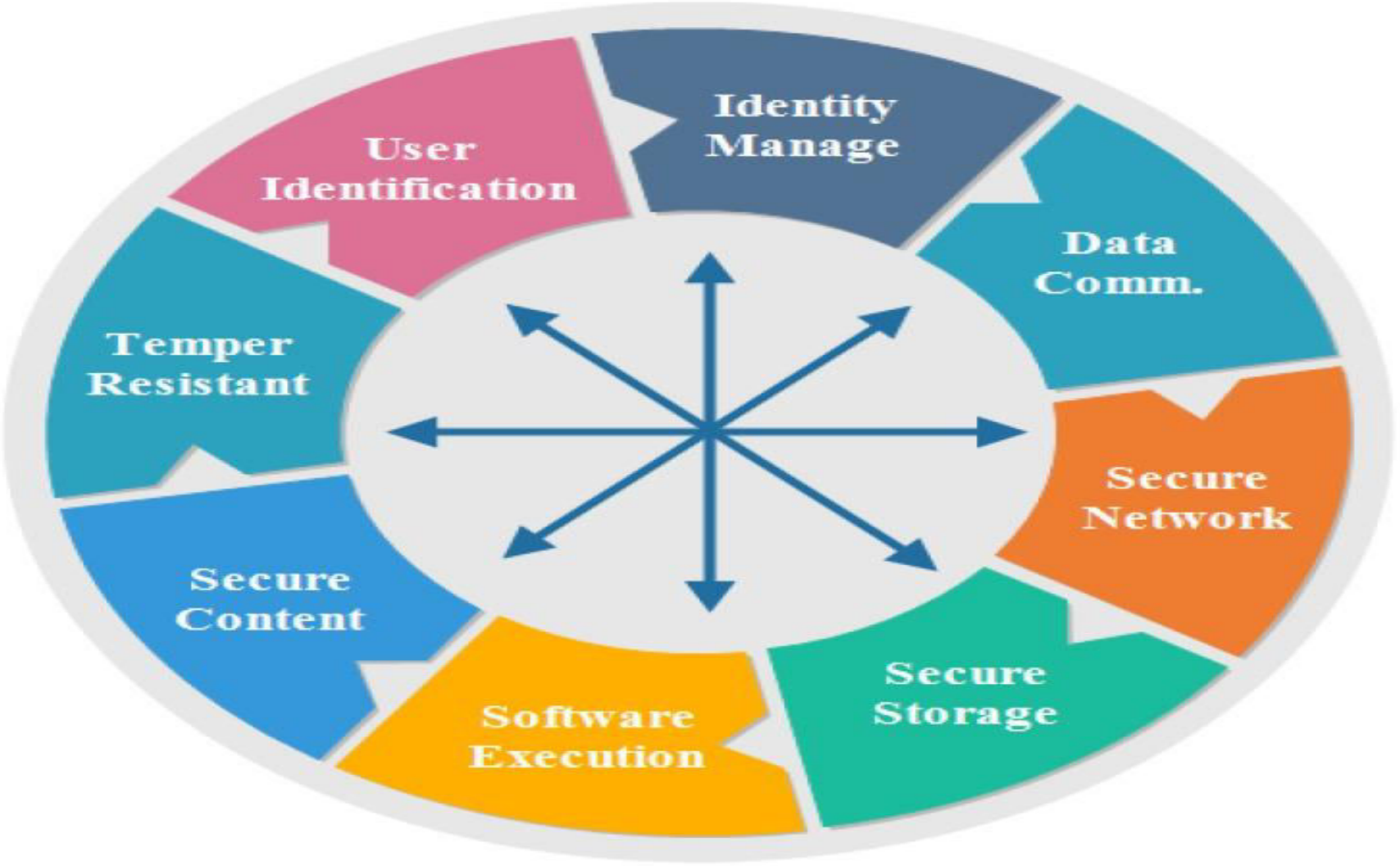
- Physical exposure
- Resource-constrained devices
- Technological heterogeneity

IOT Challenges

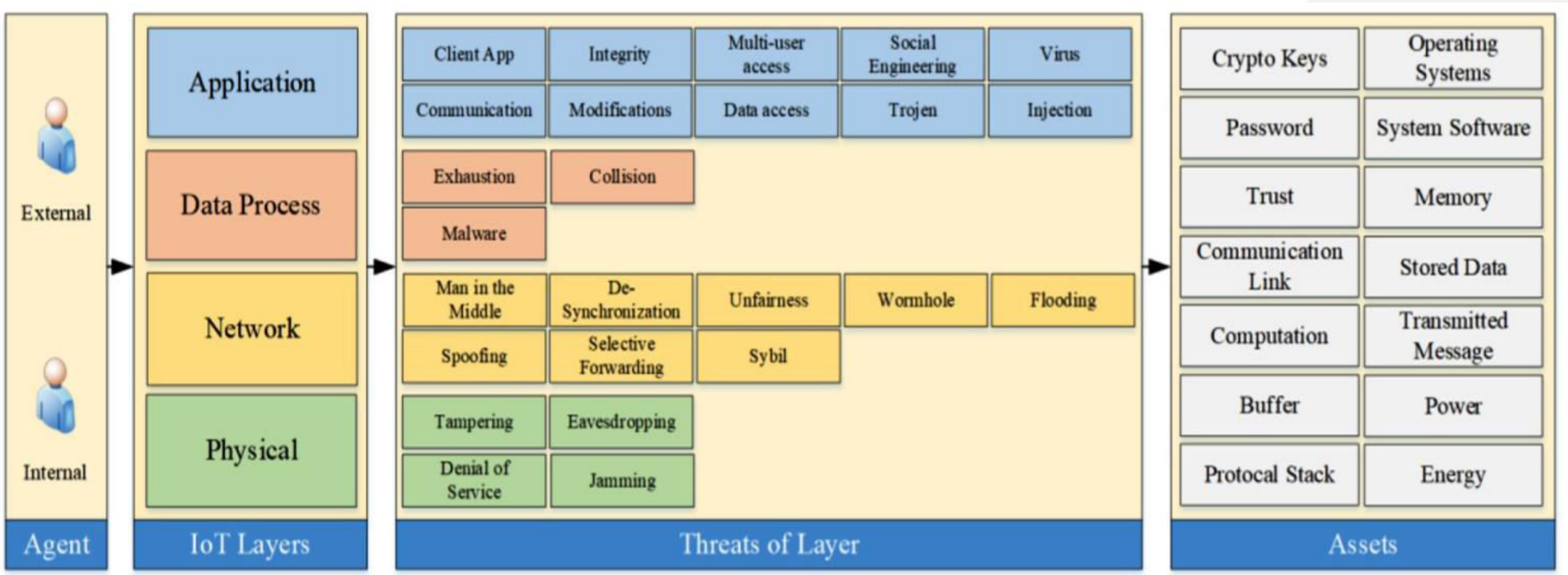


Security Challenges Facing IoT

The key security concerns in IoT



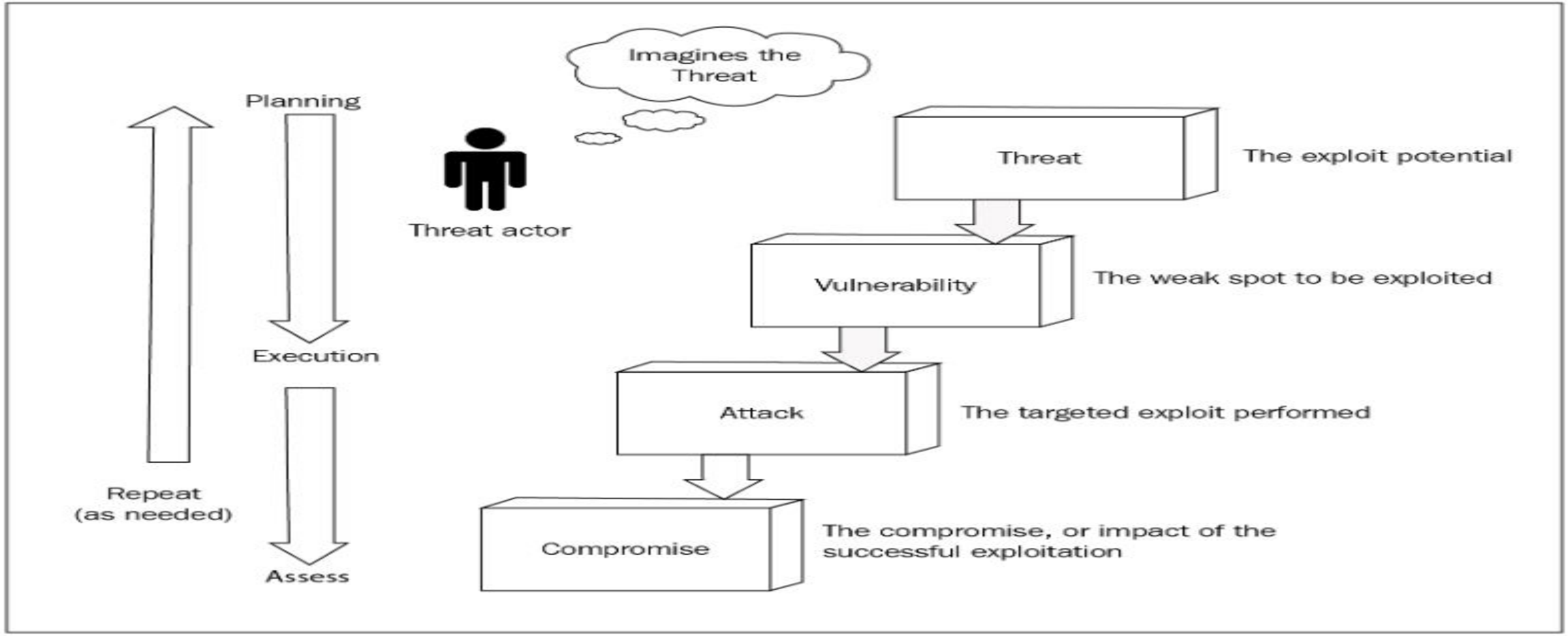
Threat classification according to IoT layers



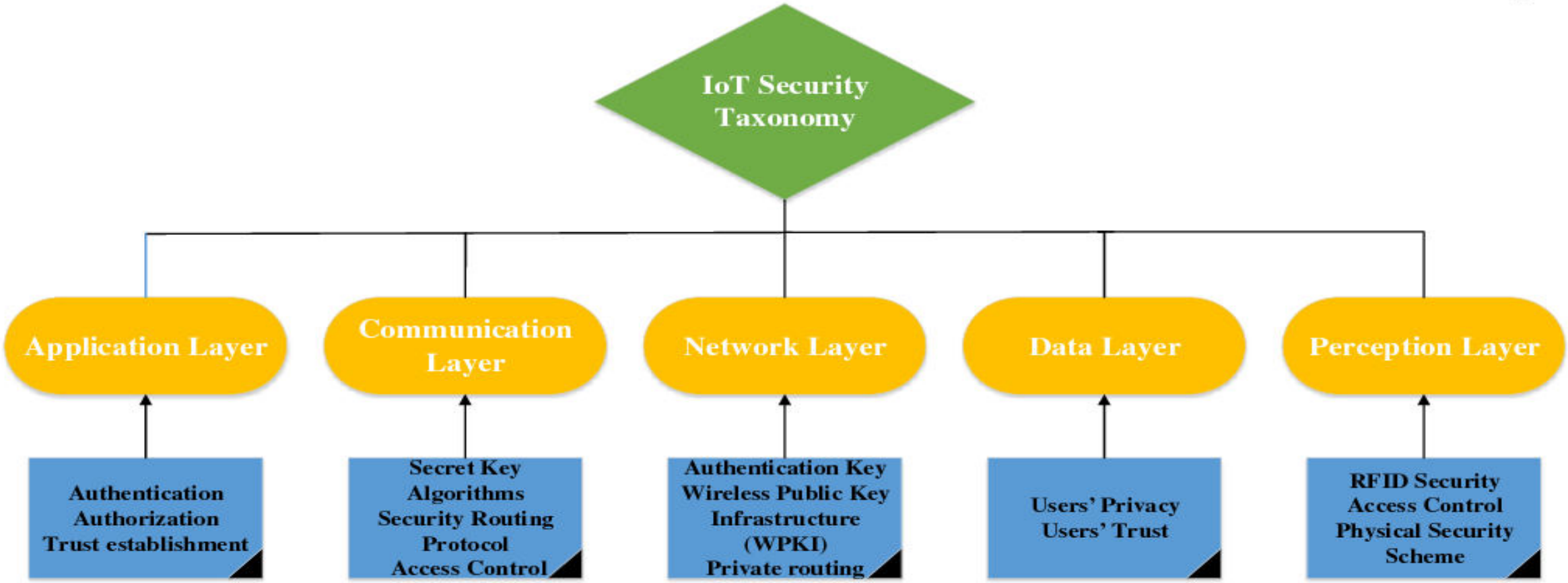
IoT Architecture and security requirements

Layer	Security Requirements
Perception	Lightweight Encryption
	Authentication
	Key Agreement
	Data Confidentiality
Network	Communication Security
	Routing Security
	Authentication
	Key Management
	Intrusion Detection
Application	Authentication
	Privacy protection
	Information Security Management

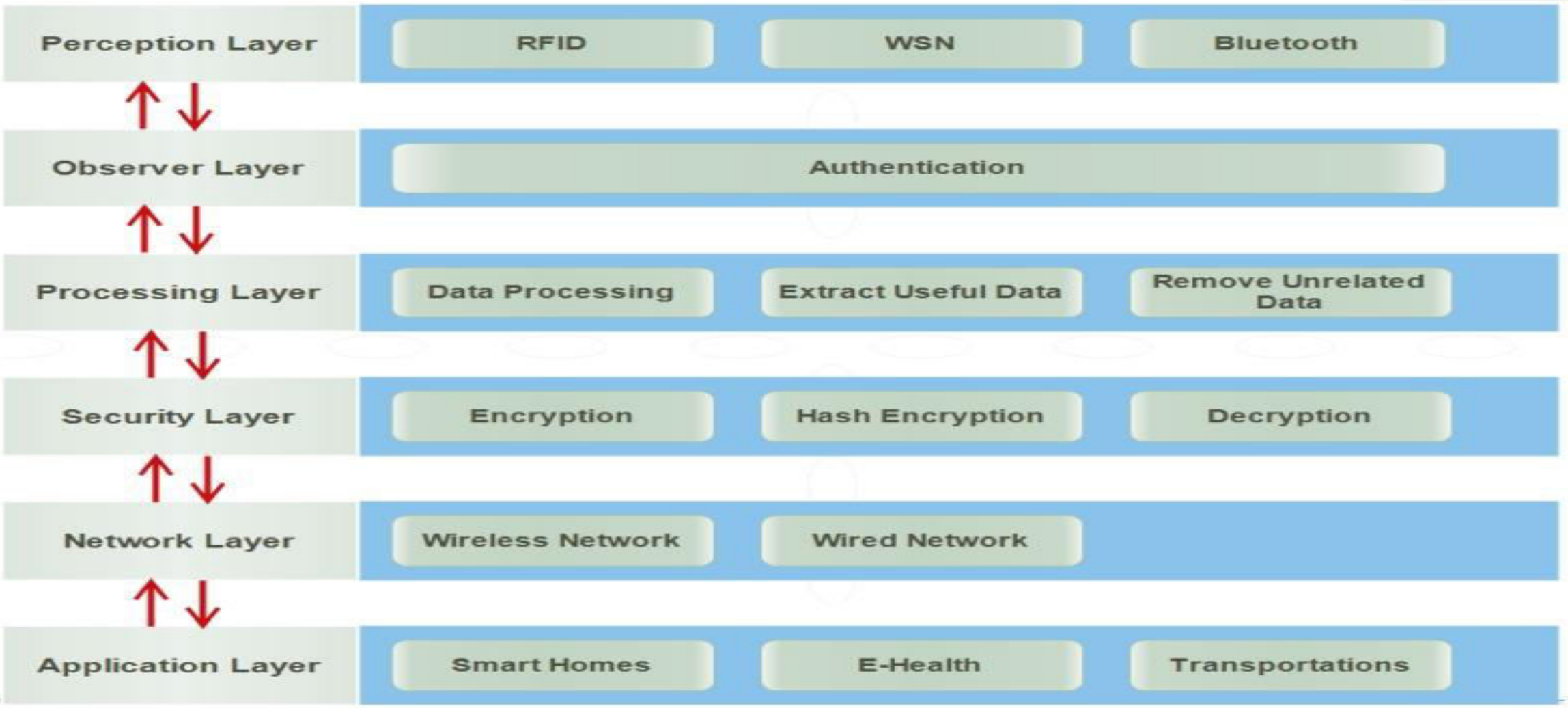
IoT Threats-A view Point



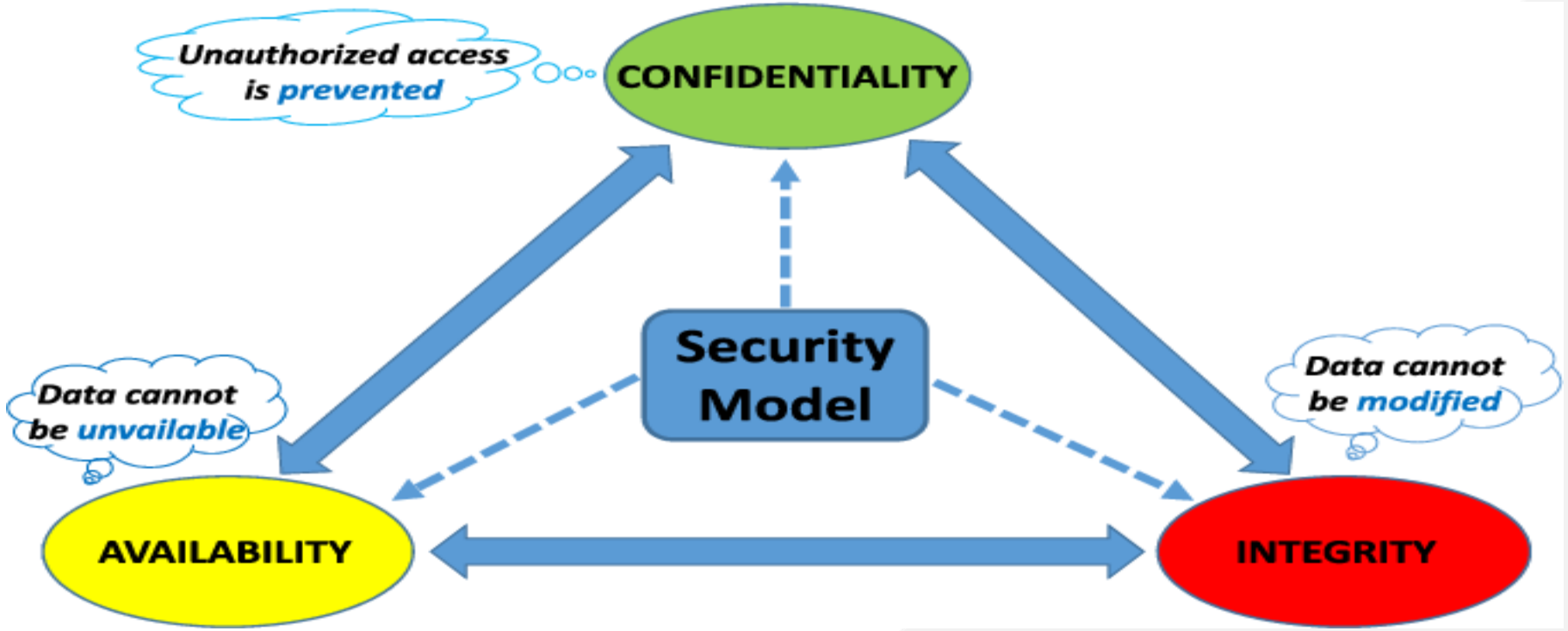
Security taxonomy of The IoT Architecture



Revised IoT layers with security embedded



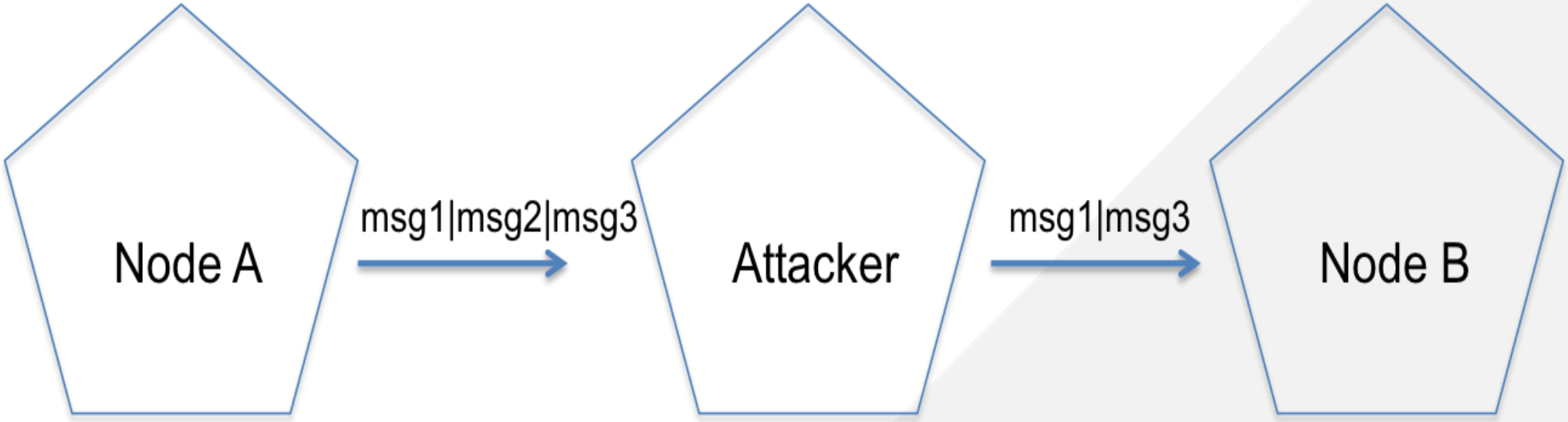
IoT Security Model



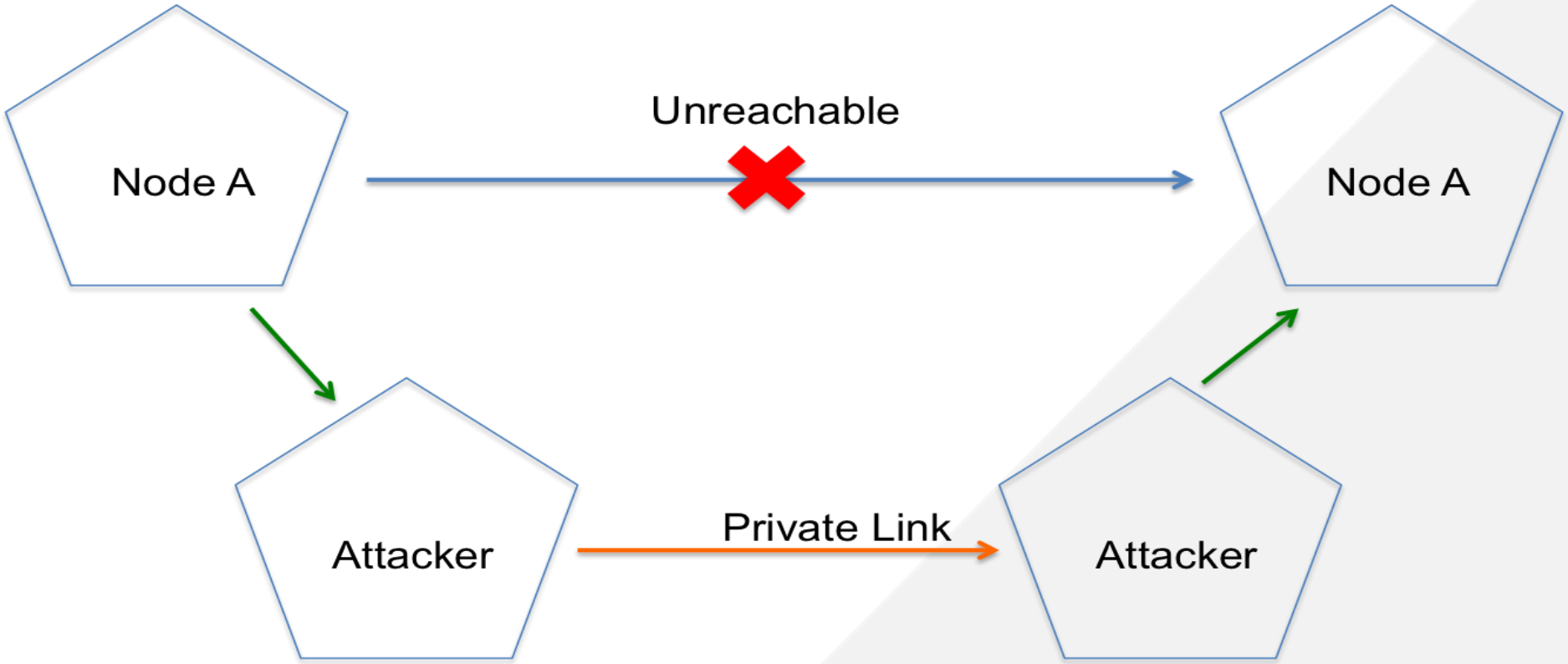
Lifecycle of a "thing

	Manufacturing	Installation/ Commissioning	Operation
Transport Layer		Eavesdropping & Man-in-the-middle	Eavesdropping & Man-in-the-middle
Network Layer			DoS attack Routing attacks
Physical Layer	Device Cloning	Substitution	DoS attack Privacy threat Extraction of security parameters

Selective Forwarding Attack



Wormhole Attack



Security Architecture & Its Requirement

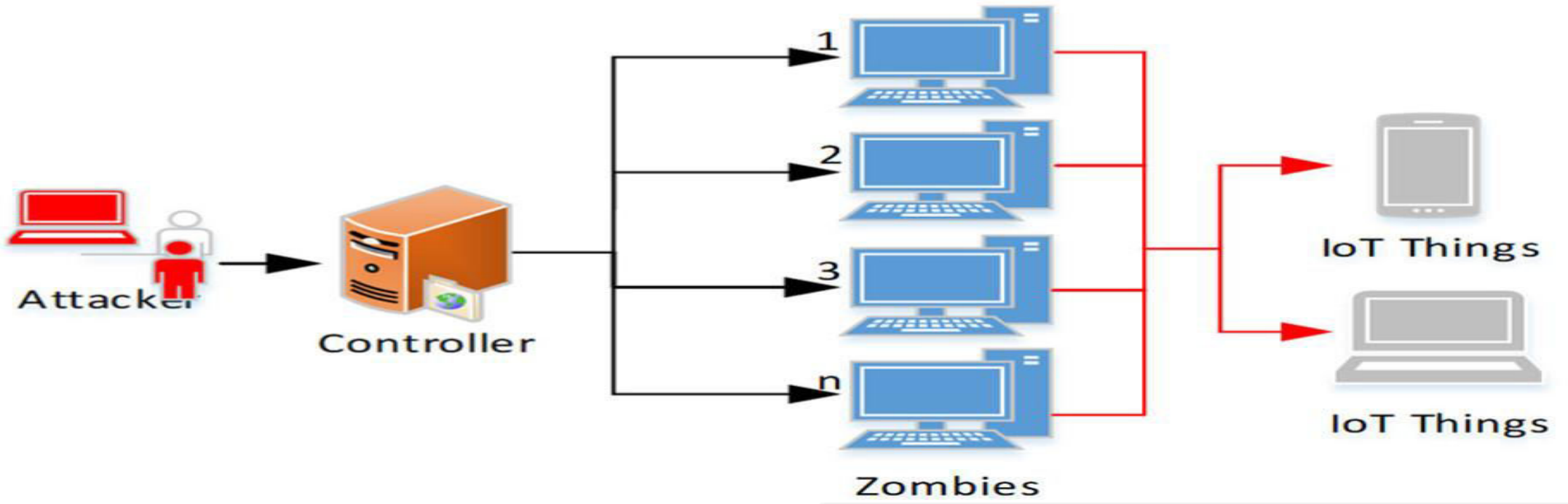
Network Layer - It carries and transmits the information collected from the physical objects through sensors.

Possible types attacks are:

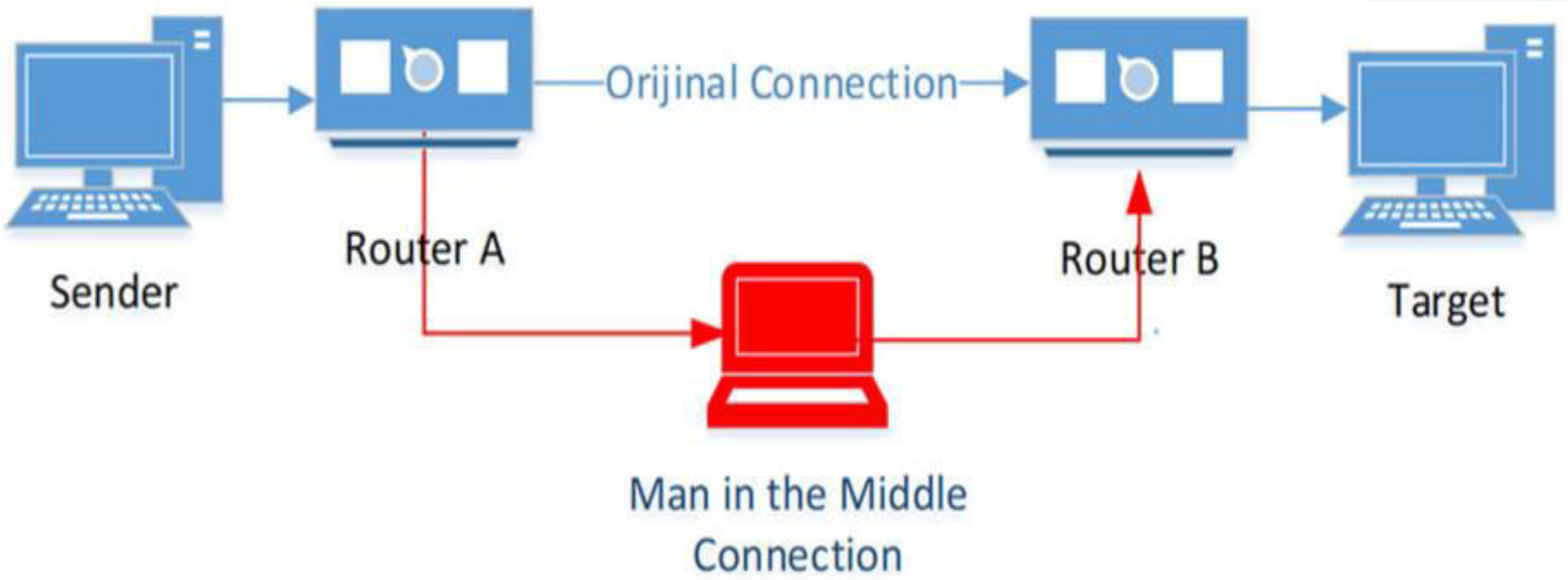
- Denial of Service (DoS) Attack
- Main-in-The-Middle (MiTM) Attack

Security Architecture & Its Requirement –type of attacks

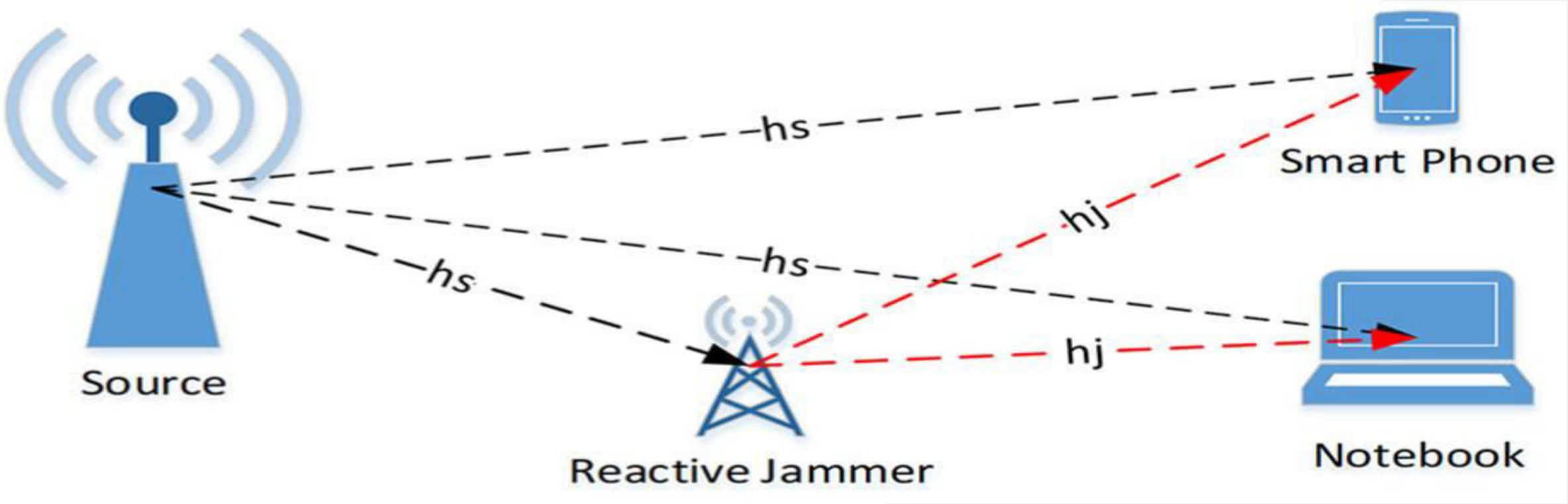
Denial of Service Attack



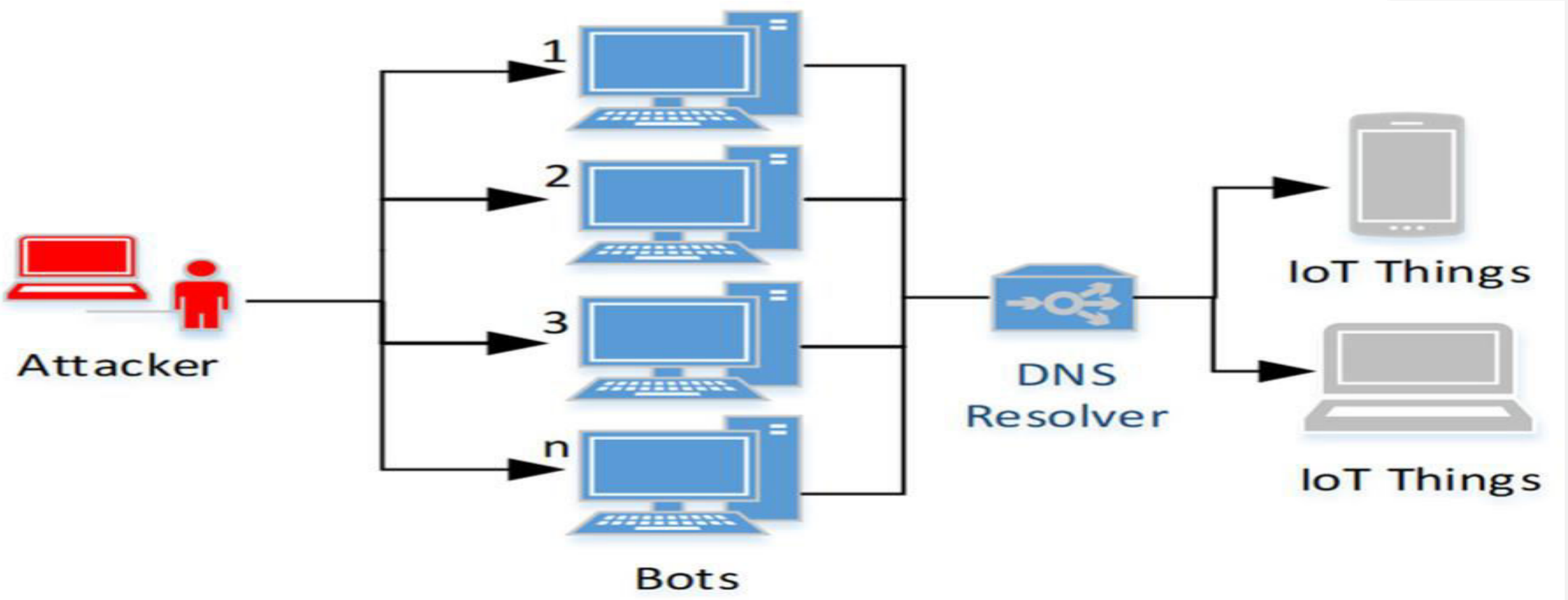
MITM attack


Orijinal Connection
Router A
Router B
Sender
Target
Man in the Middle
Connection

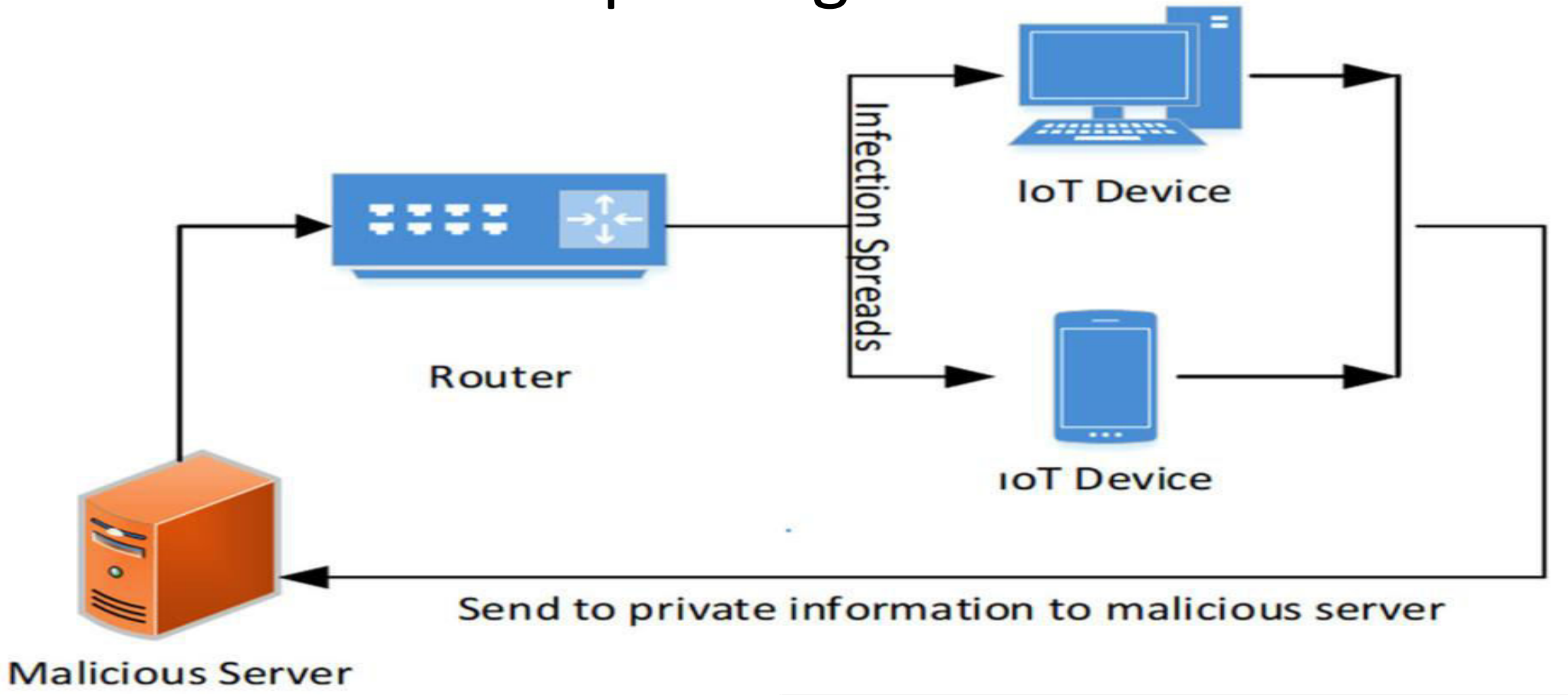
Jamming attack



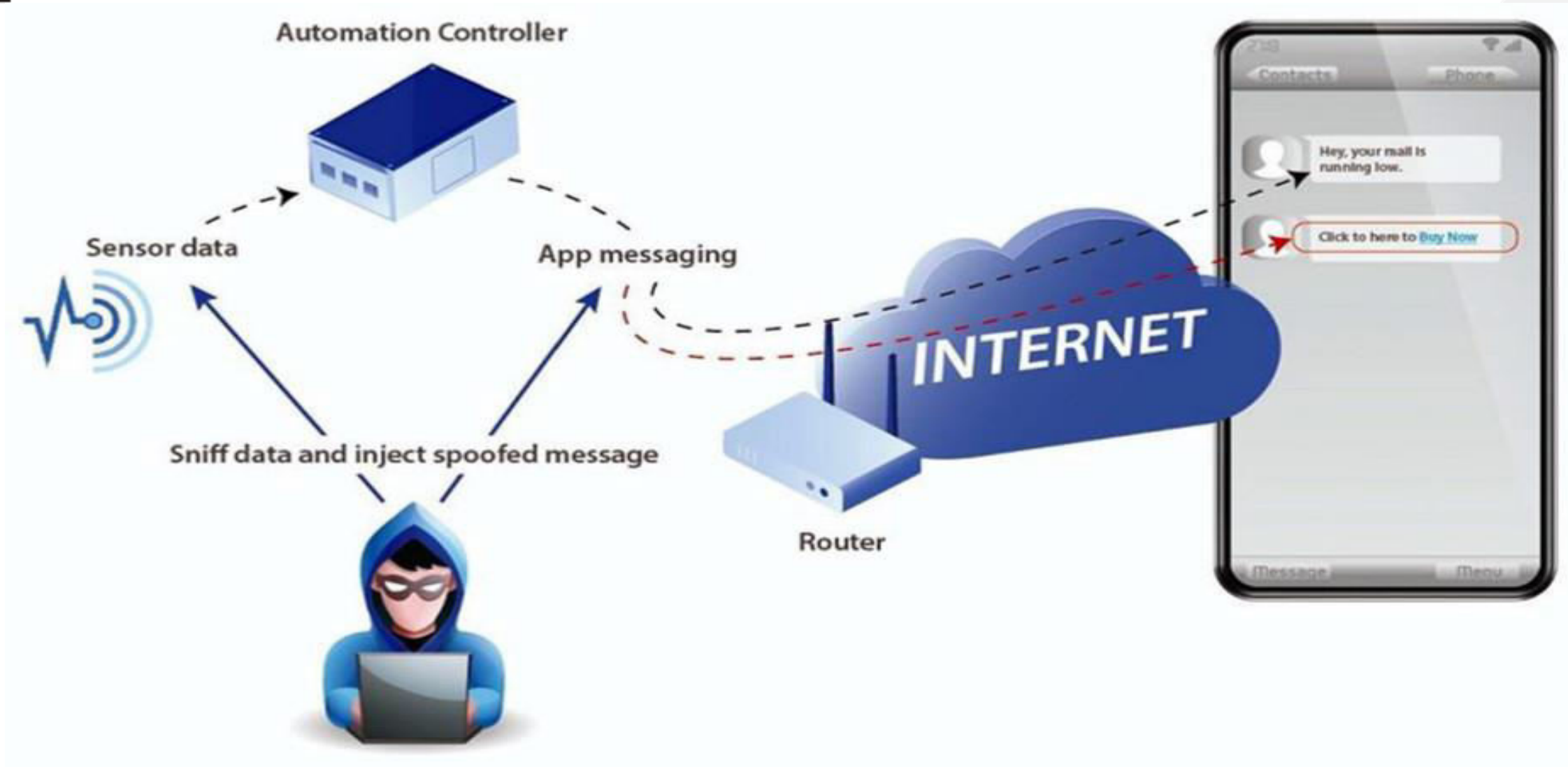
Flooding attack



Spoofing attack



Fake message–based attack to a smart IoT system



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.

Security requirements Attacks

Security Threats and Vulnerabilities at IoT End-Node

Security Threats	Description
Unauthorized Access	Due to physically capture or logic attacked, the sensitive information at the end-nodes is captured by the attacker
Availability	The end-node stops to work since physically captured or attacked logically
Spoofing attack	With malware node, the attacker successfully masquerades as IoT end-device, end-node, or end-gateway by falsifying data
Selfish threat	Some IoT end-nodes stop working to save resources or bandwidth to cause the failure of network
Malicious code	Virus, Trojan, and junk message that can cause software failure
DoS	An attempt to make a IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data Manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Security requirements Attacks

Network layer security requirements

Security Threats	Description
Data breach	Information released of secure information to an untrusted environment
Public key and private key	It comprises of keys in networks
Malicious code	Virus, Trojan, and junk message that can cause software failure
DoS	An attempt to make an IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Security requirements Attacks

Service layer security requirements

Security Threats	Description
Privacy threats	Privacy leakage or malicious location tracking
Services abuse	Unauthorized user access services or the authorized users access unsubscribed services
Identity masquerade	The IoT end-device, node, or gateway are masqueraded by attacker
Service information manipulation Repudiation	The information in services is manipulated by the attacker Denial of the operations have been done
DoS	An attempt to make an IoT end-node resource unavailable to its users
Replay attack	The attack resends the information to spoof the receiver
Routing attack	Attacks on a routing path

Security requirements

Application security requirements

Security Threats	Description
Remote configuration	Fail to configure at interfaces
Misconfiguration	Misconfiguration at remote IoT end-node, end-device, or end-gateway
Security management	Log and keys leakage
Management system	Failure of management system

Security requirements

The security requirements between layers

Security Threats	Description
Sensitive information leakage at border	The sensitive information might be not protected at the border of layers
Identity spoofing	The identities in different layers have different priorities
Sensitive information spreads between layers	Sensitive information spreads at different layers and causes information leakage

References

1. Li Da Xu, Securing Internet of Things, Algorithms, and Implementations, Elsevier
2. Chintarlapallireddy Yaswanth Simha, “Enabling Technologies for Internet of Things & It’s Security issues” ICICCS 2018

.

Home Assignment

1. Give an example of DoS security threat

THANK YOU

For queries
Email: gaurave.e9610@cumail.in