# Security Engineering

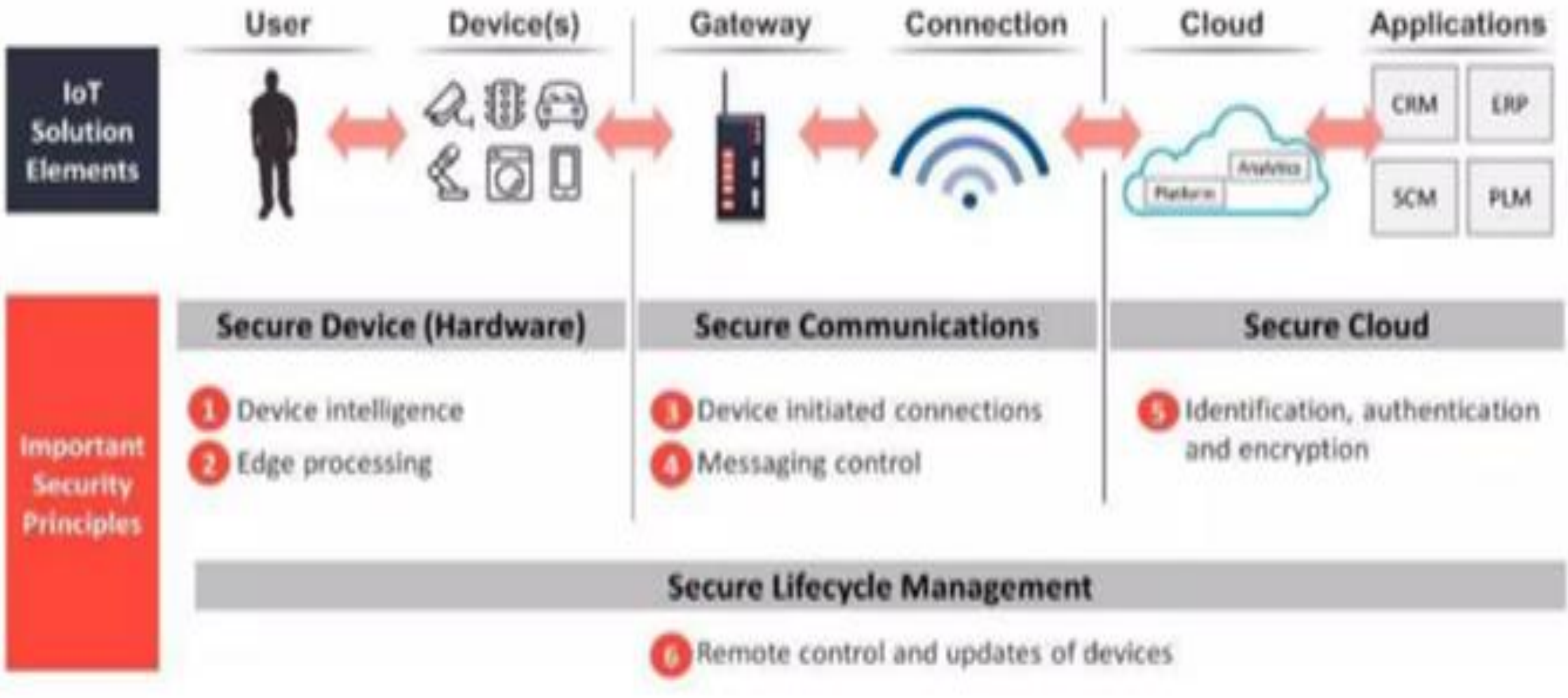
## Module V

# Contents

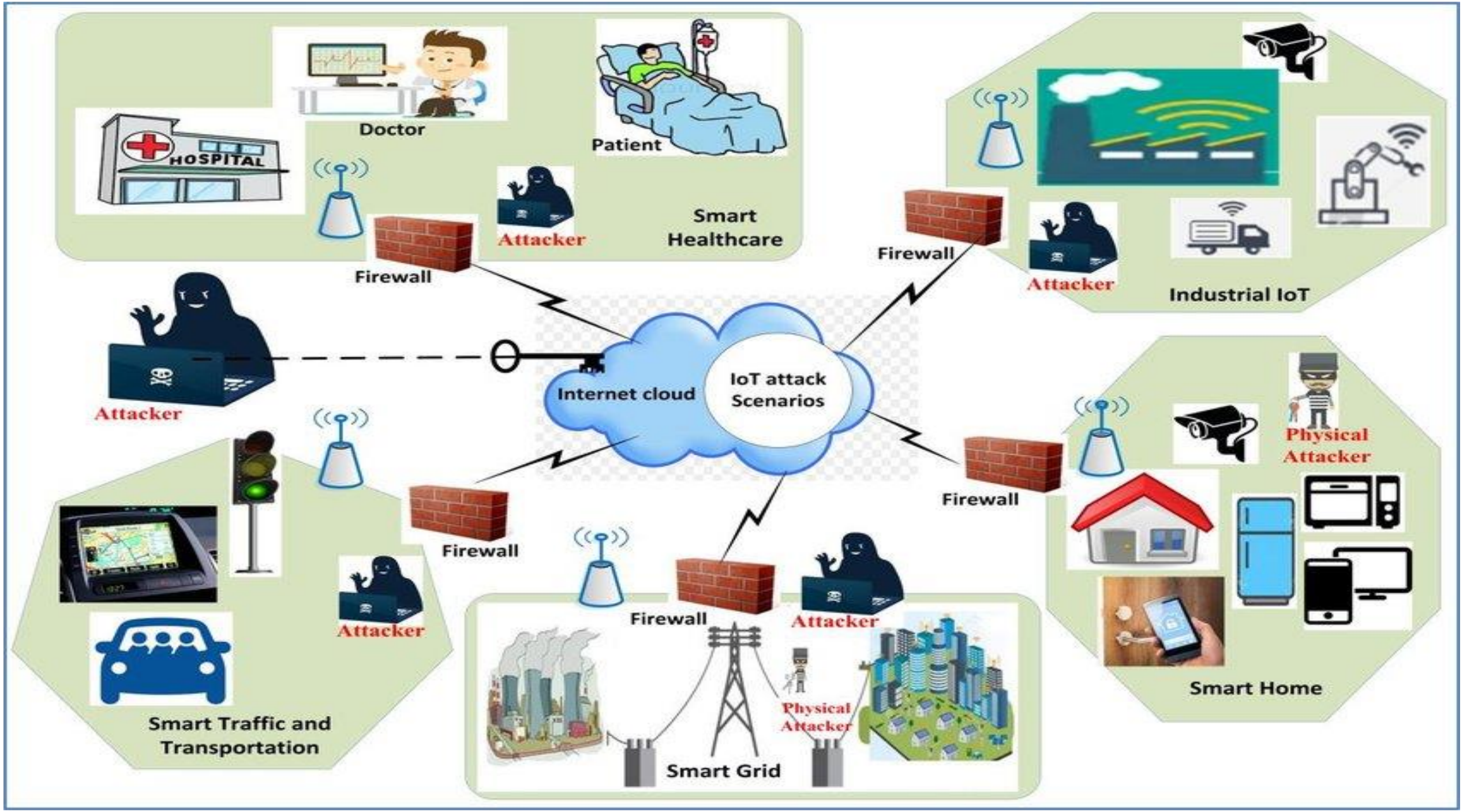
- IoT Attacks and Security Challenges,
- Threat and Mitigating Threats to IoT Systems,
- Privacy concerns - Access control, Lightweight Cryptography, Privacy in IoT

# Introduction- IOT Attacks

- The Internet of Things (IoT) promises to make our lives more convenient by turning each **physical object in our surrounding environment into a smart object** that can sense the environment, communicate with the remaining smart objects, perform reasoning, and respond properly to changes in the surrounding environment.
- However, the conveniences that the IoT brings are also associated with **new security risks and privacy issues** that must be addressed properly. Ignoring these security and privacy issues will have serious effects on the different aspects of our lives including the homes we live in, the cars we ride to work, and **even the effects that will reach our own bodies.**


IoT Solution Elements
User
Device(s)
Gateway
Connection
Cloud
Applications
CRM
ERP
SCM
PLM
Important Security Principles
Secure Device (Hardware)
1 Device intelligence
2 Edge processing
Secure Communications
3 Device initiated connections
4 Messaging control
Secure Cloud
5 Identification, authentication and encryption
Secure Lifecycle Management
6 Remote control and updates of devices

- If your **home** does not already have a smart meter, **it will soon have multiple of those meters** that are dedicated to monitor and control the power consumption, the heating, and the **lighting of your house.**
- This is not to mention the smart gadgets that will be found all over your house such as the **smart camera that notifies your smartphone during business hours** when movement is detected, the smart door that opens remotely, and the **smart fridge that notifies you when you are short of milk.**
- The level of control that an **attacker can gain by hacking those smart meters and gadgets** if the security of those devices was overlooked. In fact, **the damage caused by cyberattacks in the IoT era will have a direct impact on all the physical objects that you use in your daily life.**

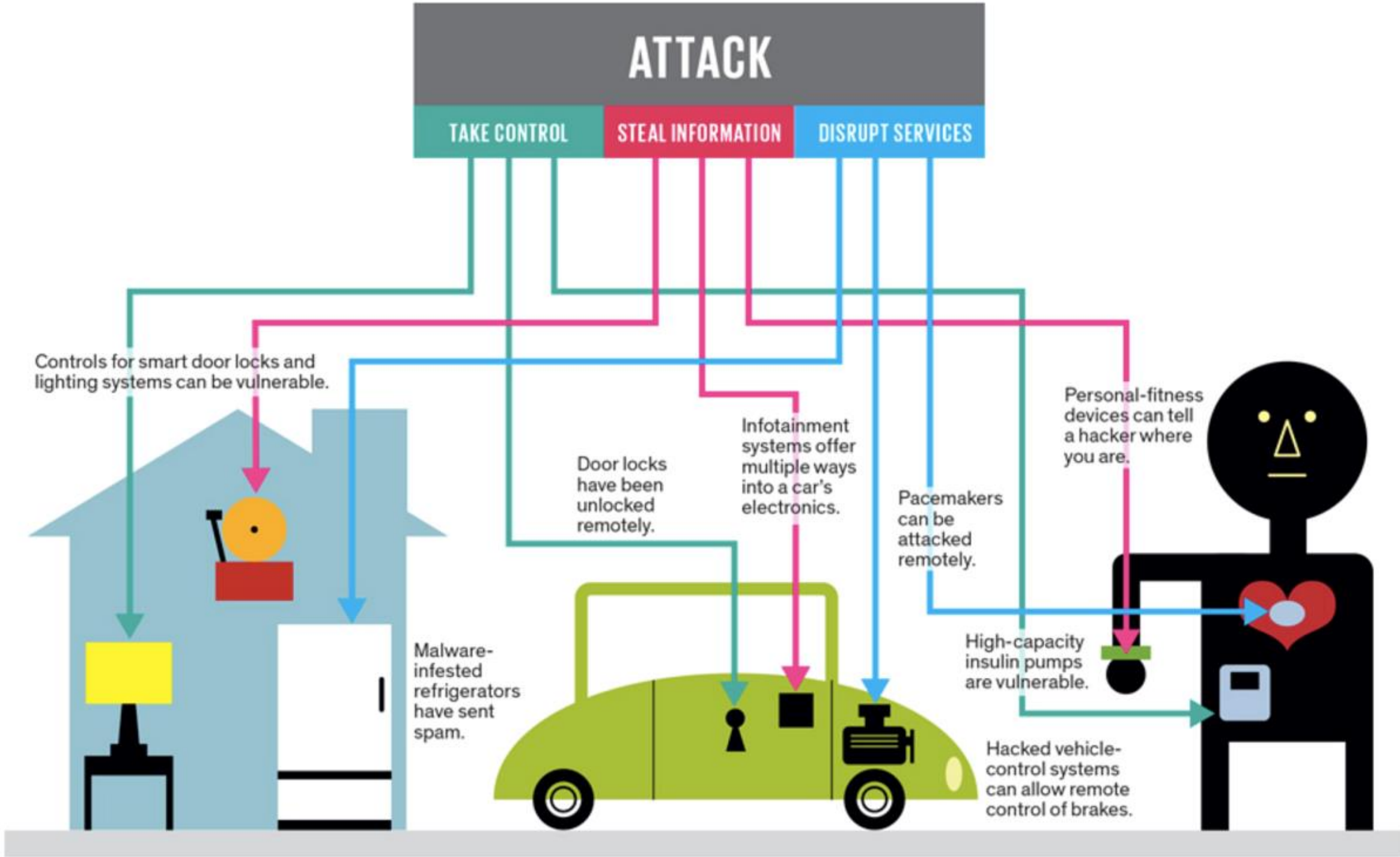

HOSPITAL
Doctor
Patient
Attacker
Firewall
Smart Healthcare
Attacker
Firewall
Attacker
Industrial IoT
Internet cloud
IoT attack Scenarios
Attacker
Firewall
Firewall
Firewall
Physical Attacker
Smart Home
Attacker
Smart Traffic and Transportation
Firewall
Attacker
Physical Attacker
Smart Grid

# Smart Car security threat

As the number of **integrated sensors for car continues to grow rapidly** and as the wireless control capabilities increase significantly over time, giving an attacker who hacks the car the ability to control the **windshield wipers, the radio, the door lock, and even the brakes and the steering wheel of your car.**

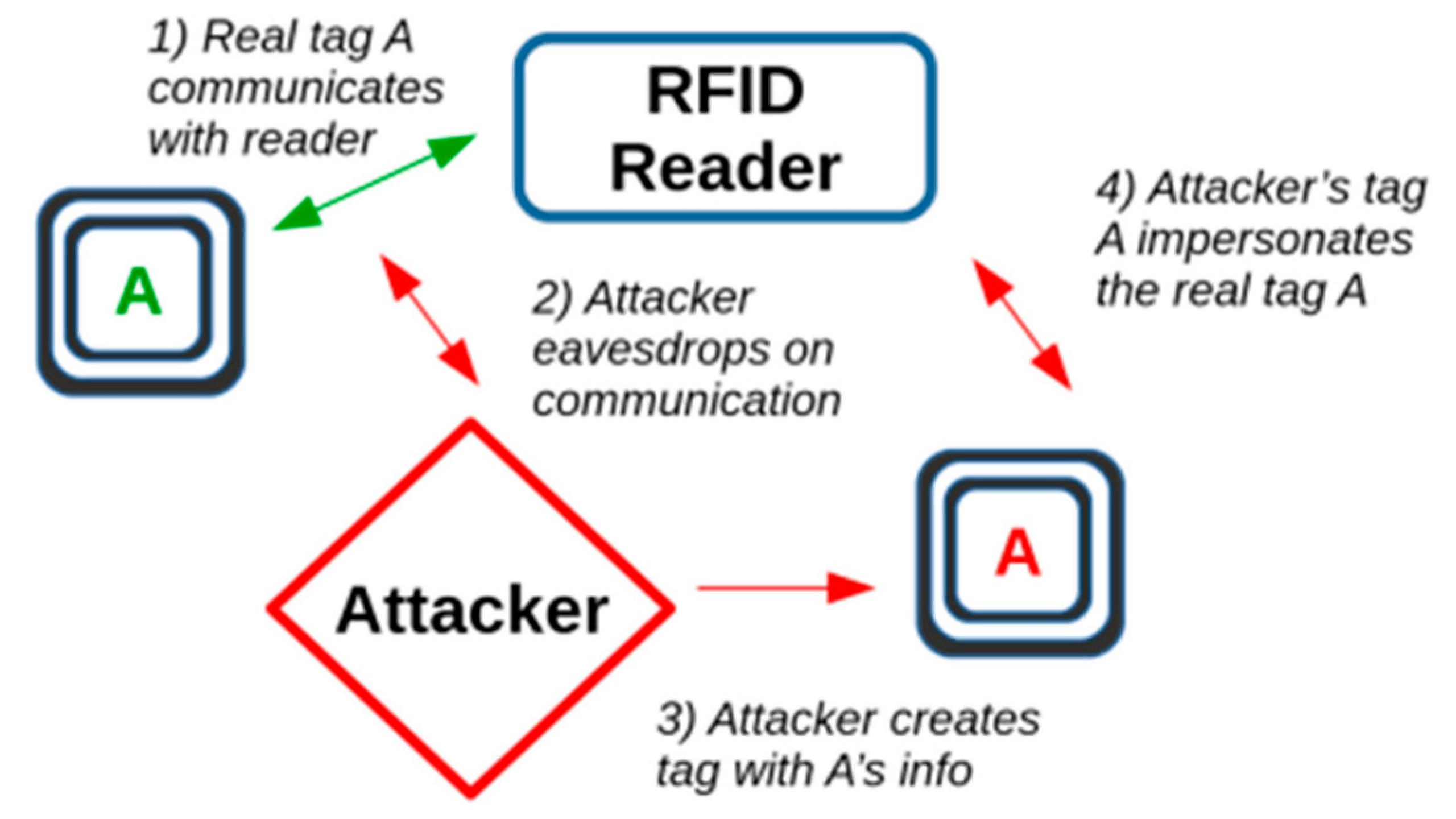
# Medical/ Human Body- Threat/Attacks

- Our bodies won’t also be safe from cyberattacks.
- In fact, researchers have shown that an attacker can control remotely the **implantable and wearable health devices** (e.g., insulin pumps and heart pacemakers) by **hacking the communication link** that connects them to the control and monitoring system.
- **This gives the attacker, for example, the ability to tune the injected insulin** dose causing serious health problems that may even cause death to patients wearing those smart health devices.


ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Pacemakers can be attacked remotely.
Personal-fitness devices can tell a hacker where you are.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.

# Business Enterprises - Attacks

- The security risks are also extremely serious when IoT devices are used in **business enterprises**. **If an attacker hacks any of those smart objects that are used in a big enterprise**, then the sensing capabilities that those **smart objects have can be used by the attacker to spy on the enterprise.**
- Such **cyberattacks** can also be used to **steal sensitive information such as the company earnings report and credit card information.**
- In fact, these stealing attacks are common in big enterprises such as the largest financial hacking case in the US history, which took place in 2013, where a group of **five hackers stole $160 million from credit cards** and over hundreds of millions in criminal loot.


1) Real tag A communicates with reader
RFID Reader
A
2) Attacker eavesdrops on communication
4) Attacker's tag A impersonates the real tag A
Attacker
A
3) Attacker creates tag with A's info

# IoT Security Challenges

- IoT has unique characteristics and constraints when it comes to designing **efficient defensive mechanisms against cyber-security threats** that can be summarized by:

1. Multiple Technologies
2. Multiple Verticals
3. Scalability
4. Big Data
5. Resource Limitations
6. Remote Locations
7. Mobility
8. Delay-Sensitive Service

# IoT Security Challenges

1. ***Multiple Technologies*:** IoT combines multiple technologies such as **radio-frequency identification (RFID)**, **wireless sensor networks, cloud computing, virtualization**, etc. Each of these technologies has its own vulnerabilities. The problem with the IoT paradigm is that one must secure the chain of all of those technologies as the security resistance of an IoT application will be judged based on its weakest point which is usually referred to by **Achilles' heel.**

- **For example**, consider a **smart home system** that incorporates various IoT technologies such as **RFID for access control, wireless sensor networks for environmental monitoring, and cloud computing for data storage and processing**. Each of these technologies has its unique vulnerabilities.

# IoT Security Challenges

- In this scenario, if the **RFID access control system is poorly implemented** and susceptible to cloning or **unauthorized access**, it becomes the weakest point in terms of security. Despite having robust security measures in the wireless sensor networks and cloud computing components, the overall security resistance of the IoT application will be judged based on the **vulnerability of the RFID system.**
- In such cases, **securing the entire IoT chain becomes crucial**. **It involves implementing appropriate security measures for each technology, addressing their respective vulnerabilities, and ensuring seamless integration and cooperation between the various components**. Focusing solely on one technology's security while neglecting others leaves the system exposed to potential attacks and compromises the overall security posture.

# IoT Security Challenges

***2. Multiple Verticals*:** The IoT paradigm will have numerous applications (also called verticals) that span eHealth, industrial, smart home gadgets, smart cities, etc. The security requirements of each vertical are quite different from the remaining verticals.

- For example, let's consider two IoT verticals: **eHealth and industrial systems**. In the **eHealth vertical, the security requirements focus heavily on protecting sensitive patient data**, ensuring the confidentiality and integrity of medical records, and maintaining the privacy of individuals' health information. **The eHealth vertical may require strong authentication mechanisms, encryption protocols, and stringent access control** to protect against **data breaches and unauthorized access** to medical devices or patient records.

- On the other hand, **in the industrial vertical**, the security concerns revolve around **protecting critical infrastructure, such as manufacturing plants or power grids, from cyber threats**. Industrial systems may require **robust network segmentation, intrusion detection systems, and secure remote access protocols** to prevent unauthorized access and potential disruptions to operations.
- As evident from this example, **the security requirements for eHealth and industrial verticals differ significantly due to the nature of the data being handled. Similar variations exist among other IoT verticals like smart home gadgets, smart cities, and more, as they cater to different purposes and use cases.**
- Security engineers and practitioners need to consider the specific needs of each vertical, **develop tailored security solutions, and implement appropriate security measures to protect against the unique threats** associated with that particular domain.

# IoT Security Challenges

**3. Scalability:** The number of IoT devices or sensors are increasing day by day. Developing efficient defensive mechanisms becomes difficult with this.

- For example, consider a smart city deployment with numerous IoT devices and sensors spread across various locations. These devices may include **smart streetlights, environmental sensors, traffic monitoring systems**, and more. **The number of endpoints in such a deployment can quickly reach hundreds of thousands or even millions.**

- In this scenario, **scalability becomes a critical consideration for IoT security**. The defensive mechanisms employed must be able to handle the **increasing number of devices and endpoints efficiently**. Traditional centralized approaches, which rely on a single point of control or management, **may struggle to scale effectively when dealing with such large-scale IoT deployments.**
- To address the scalability challenge, **practical decentralized defensive security mechanisms are needed**. These mechanisms distribute security functions across the IoT network, allowing for more **efficient and scalable management**. This can involve implementing distributed authentication, encryption, and access control mechanisms, as well as **leveraging edge computing capabilities to offload processing tasks closer to the devices.**

# IoT Security Challenges

***4. Big Data:*** **The vast number of smart objects and their associated sensors will generate enormous amounts of data over time, requiring efficient defensive mechanisms to secure these large data streams.**

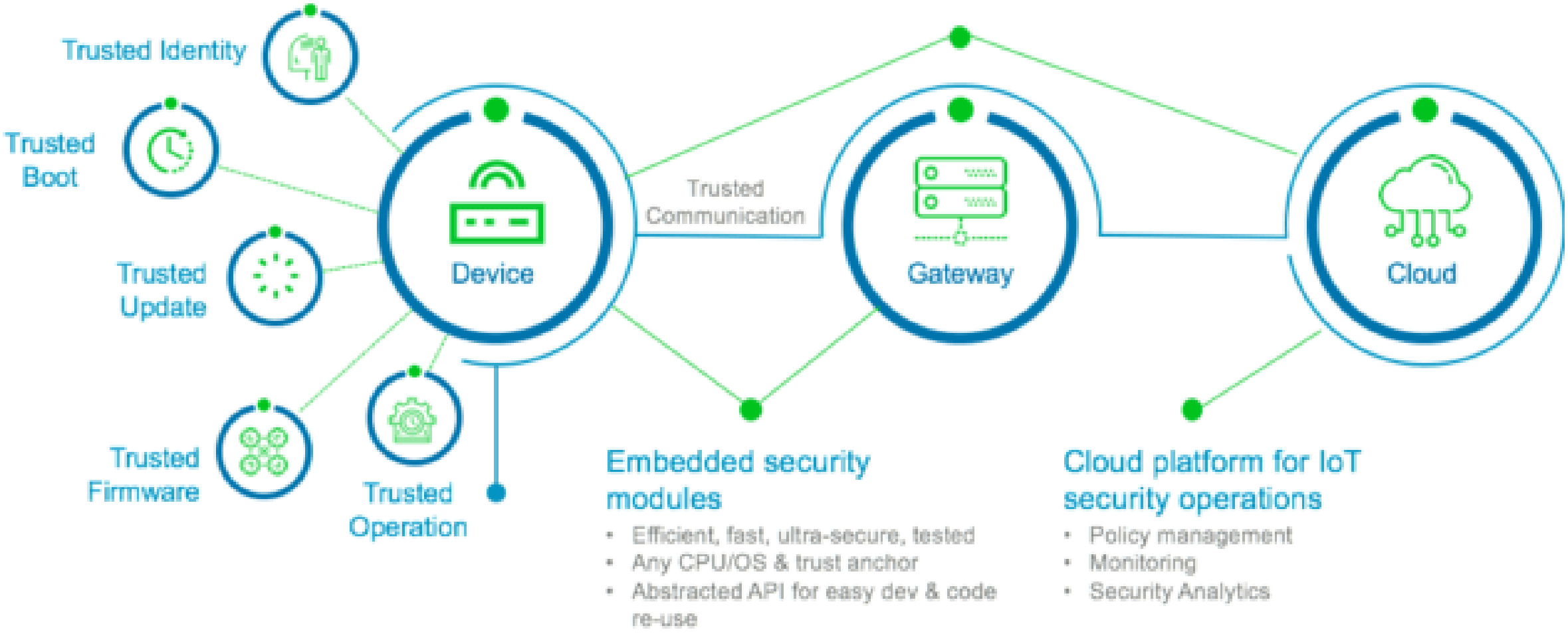
***5. Resource Limitations:*** **IoT end devices often have limited resources such as CPU, memory, storage, battery, and transmission range. These limitations make them vulnerable to denial of service (DoS) attacks, as attackers can easily overwhelm the device's resources, leading to service disruptions. Furthermore, the resource constraints of these devices pose challenges for developing security protocols, particularly considering that traditional cryptography techniques are computationally expensive.**

***6. Remote Locations:*** **In certain IoT verticals like smart grid, railways, and roadsides, IoT devices, especially sensors, are deployed in unmanned and hard-to-reach locations. Attackers can exploit these devices without detection. To address this challenge, cyber and physical security monitoring systems need to be installed in secure locations. These systems should be able to operate in extreme environmental conditions, fit into small spaces, and facilitate remote updates and maintenance to avoid costly and delayed visits by network technicians.**

# IoT Security Challenges

***7. Mobility:*** Smart objects are expected to **change their location** often in the IoT paradigm. This adds extra difficulties when **developing efficient defensive mechanisms** in such dynamic environments.

***8. Delay-Sensitive Service:*** The majority of IoT applications are expected to be **delay-sensitive**, and thus one should protect the different **IoT components from any attack** that may **degrade their service time** or may cause a service disruption.




A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack

# THE IoT ATTACK SURFACE

## What are IoT threat actors after?

### Information

The IoT holds an abundance of information that can be critical, private, or sensitive, depending on the environment or industry.

### Lateral movement

A single exposed IoT device can enable a cybercriminal to gain access to an enterprise's corporate or industrial network, which in turn can allow for other attacks like sabotage.

### Monetary gain

IoT attacks can prove profitable for threat actors, who can choose to sell stolen data or seek payment to relinquish control of compromised assets.

### Attack base

Hackers can weaponize IoT devices for attacks that can be spread outward or deeper into the main infrastructure. They can also build a secure channel node to mask their traffic as legitimate.

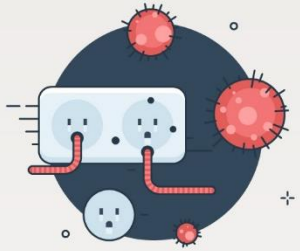
## What are common IoT attacks?

### Vulnerability exploits

The many components used in IoT devices mean they can have any number of vulnerabilities that can be exploited by attackers if not immediately patched.

### Malware

Malware like trojans, backdoors, and ransomware can be deployed through vulnerable applications, devices, firmware, protocols, and other components of IoT systems.



### DoS and DDoS

The growing number of IoT devices and their connectivity make the IoT susceptible to and advantageous for botnet attacks such as those used for distributed denial of service (DDoS).

### Man-in-the-middle attacks

Unsecure protocols and networks can allow attackers to position themselves between communication channels.

### Physical tampering

Deployment in poorly secured areas can subject devices to tampering like circuit modification and even replacement with unsecure devices.

### Eavesdropping and information theft

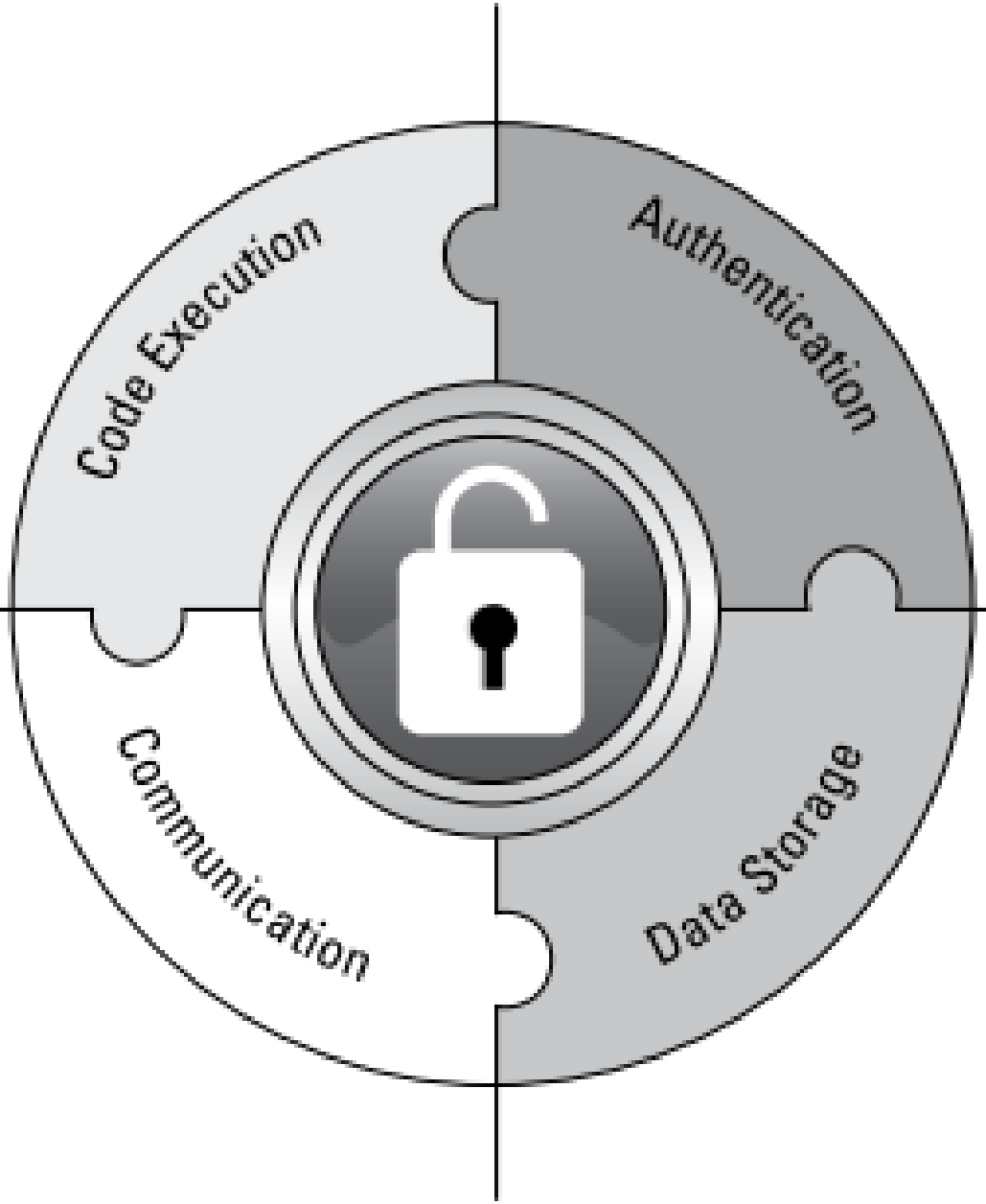
The transmission and storage of data in IoT systems can be taken advantage of by attackers to gain access to critical information and even to carry out real-time monitoring.

How can I make sure the device functions as intended?

Protect the data in process

How to ensure only authorized devices are connected to the network?

Protect access to the data




How do I protect my communications from intrusions and spying?

Protect the data in transit

How do I ensure critical assets in the device are not compromised?

Protect the data at rest

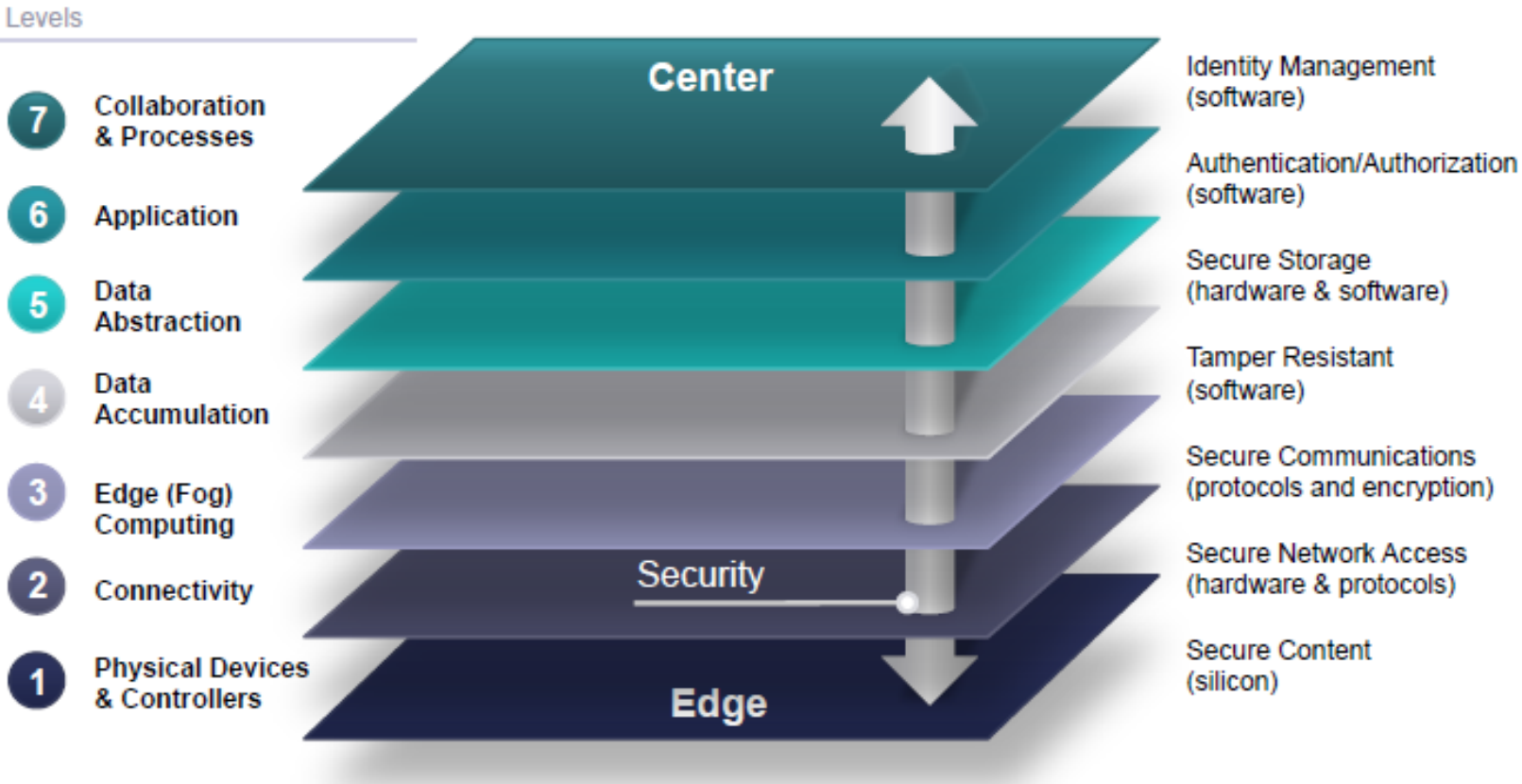
# IoT Security Requirements

- ***Confidentiality*:** Ensures that the exchanged messages can be understood only by the **intended entities.**
- ***Integrity*:** Ensures that the exchanged messages were not **altered/tampered by a third party.**
- ***Authentication***: Ensures that the entities involved in any operation are who they **claim to be**. An attack usually targets this requirement where an **entity claims to be another identity.**
- ***Availability*:** Ensures that the service is **not interrupted**. **Denial of service attacks** target this requirement as they cause **service disruption**. Attacks targeting the system availability are considered Denial of service attacks (DOS) which aim to disturb the data transfer in order to make the resources unavailable.
- ***Authorization*:** Ensures that entities have the required control permissions to perform the **operation they request to perform.**

# IoT Security Requirements

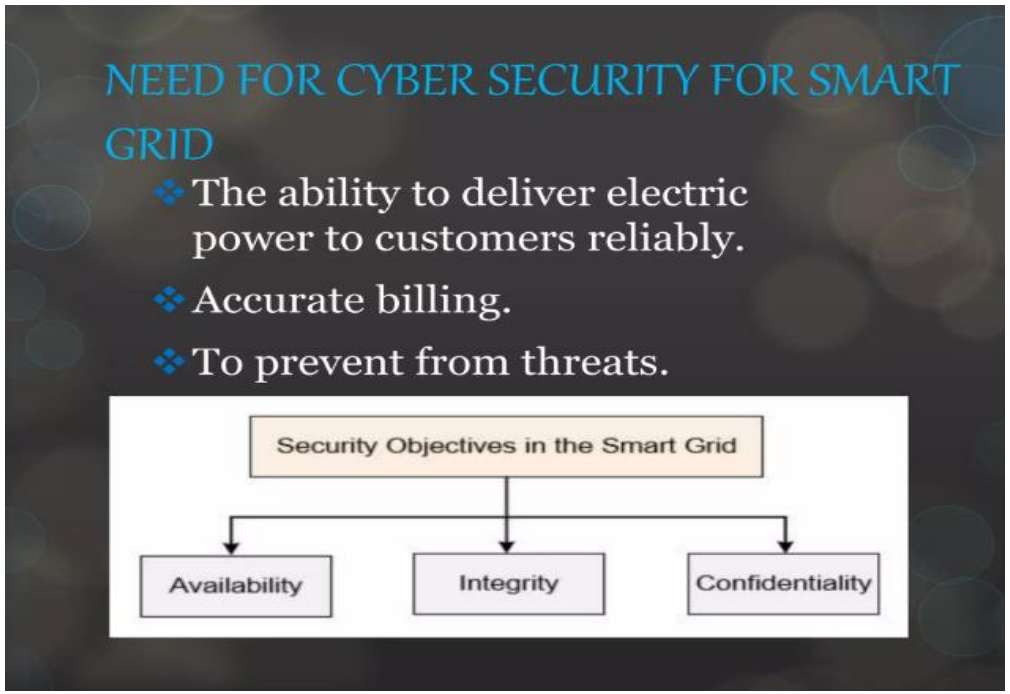
- ***Freshness*:** Ensures that the data is fresh. Replay attacks target this requirement **where an old message is replayed in order to return an entity into an old state.**
- ***Non-repudiation*:** Ensures that an entity can't deny an action **that it has performed.**
- ***Forward Secrecy*:** Ensures that when an object leaves the network, it will not understand the **communications that are exchanged after its departure.**
- ***Backward Secrecy*:** Ensures that any new object that joins the network will not be able to understand the **communications that were exchanged prior to joining the network.**

# Internet of Things Reference Model: Security




## Cyber Security of Smart Grid

- Traditionally, power grid automation systems have been physically isolated from the corporate network.
- This has been changing, perhaps due to the cost effectiveness of utilizing public networks.
- Using public networks considerably increases the vulnerability of power grids to cyber attacks by increasing the exposure surface of these networks.



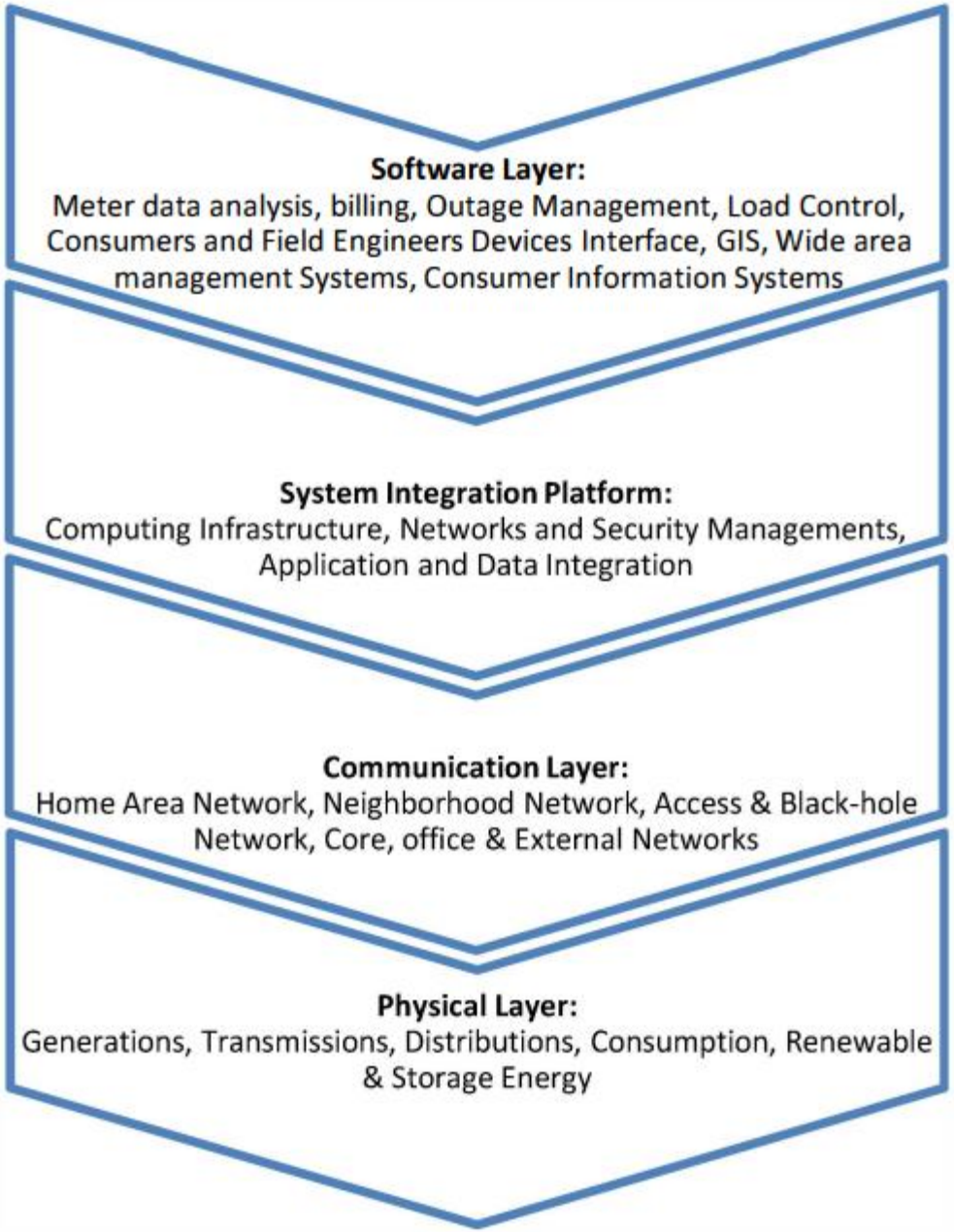




Figure 1. Smart grid conceptual model.

# Threat and Mitigating Threats to IoT Systems

- Threats to IoT systems pose **significant challenges** in maintaining the security and integrity of connected devices, networks, and the data they generate.
- As IoT deployments continue to grow in scale and complexity, it becomes **crucial to understand the various threats that can compromise the confidentiality, integrity, and availability of IoT systems**. Mitigating these threats is essential to ensure the reliable and secure operation of IoT deployments.

# Threat and Mitigating Threats to IoT Systems

**Device susceptibility or weakness:**

**Threat:** IoT devices often have limited resources and may have **weakness in their firmware or software**, making them susceptible to exploitation.

**Mitigation:** **Regular firmware and software updates** should be applied to IoT devices to patch known weakness. Additionally, implementing secure coding practices during the **development phase can reduce** the **likelihood of introducing** vulnerabilities.

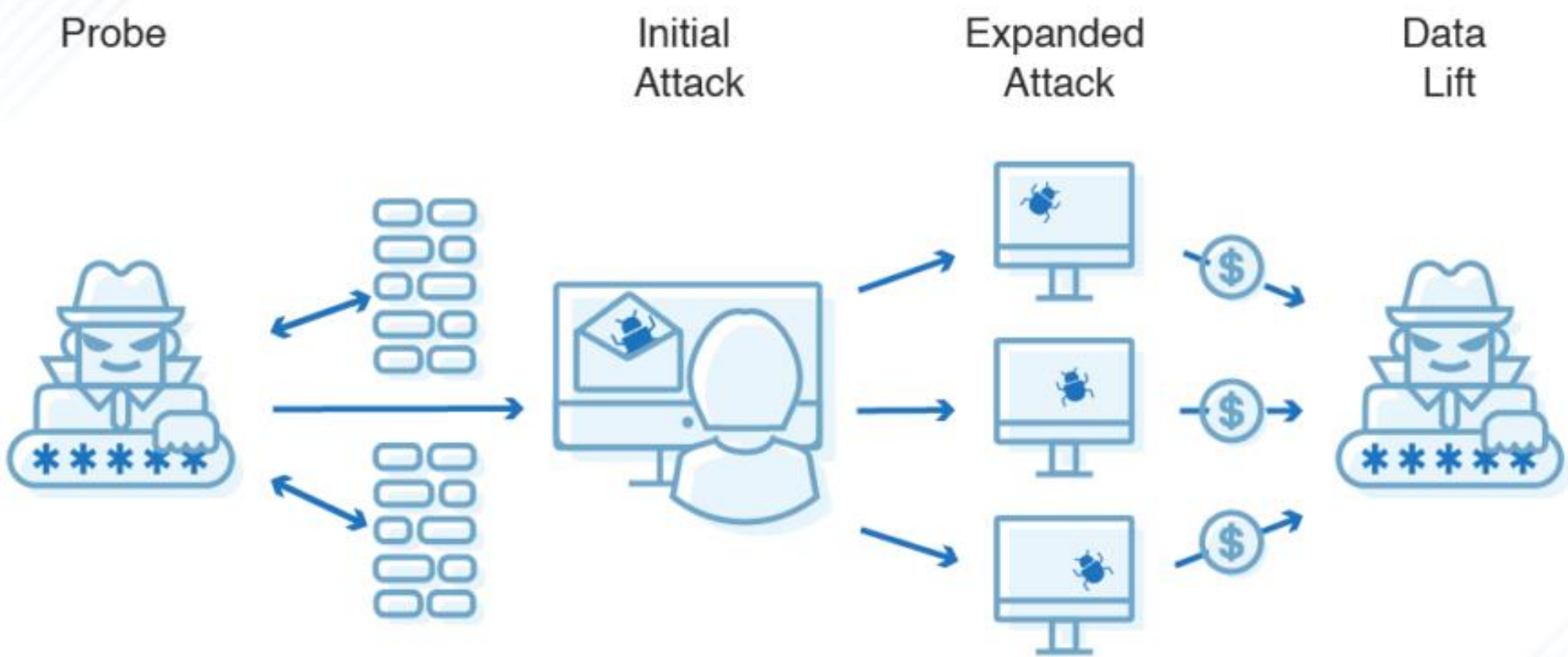

# Top Vulnerabilities of IoT Devices

# Threat and Mitigating Threats to IoT Systems

## Unauthorized Access and Data Breaches:

- **Threat: Attackers may attempt to gain unauthorized access to IoT devices** or intercept sensitive data being transmitted within IoT systems, **leading to privacy breaches** or unauthorized control over devices.
- **Mitigation:** Strong authentication mechanisms, such as **multi-factor authentication, secure passwords, or biometric authentication**, should be implemented to prevent unauthorized access. Encrypting communication channels using protocols like **Transport Layer Security (TLS) or virtual private network** (VPNs) helps protect data from interception.

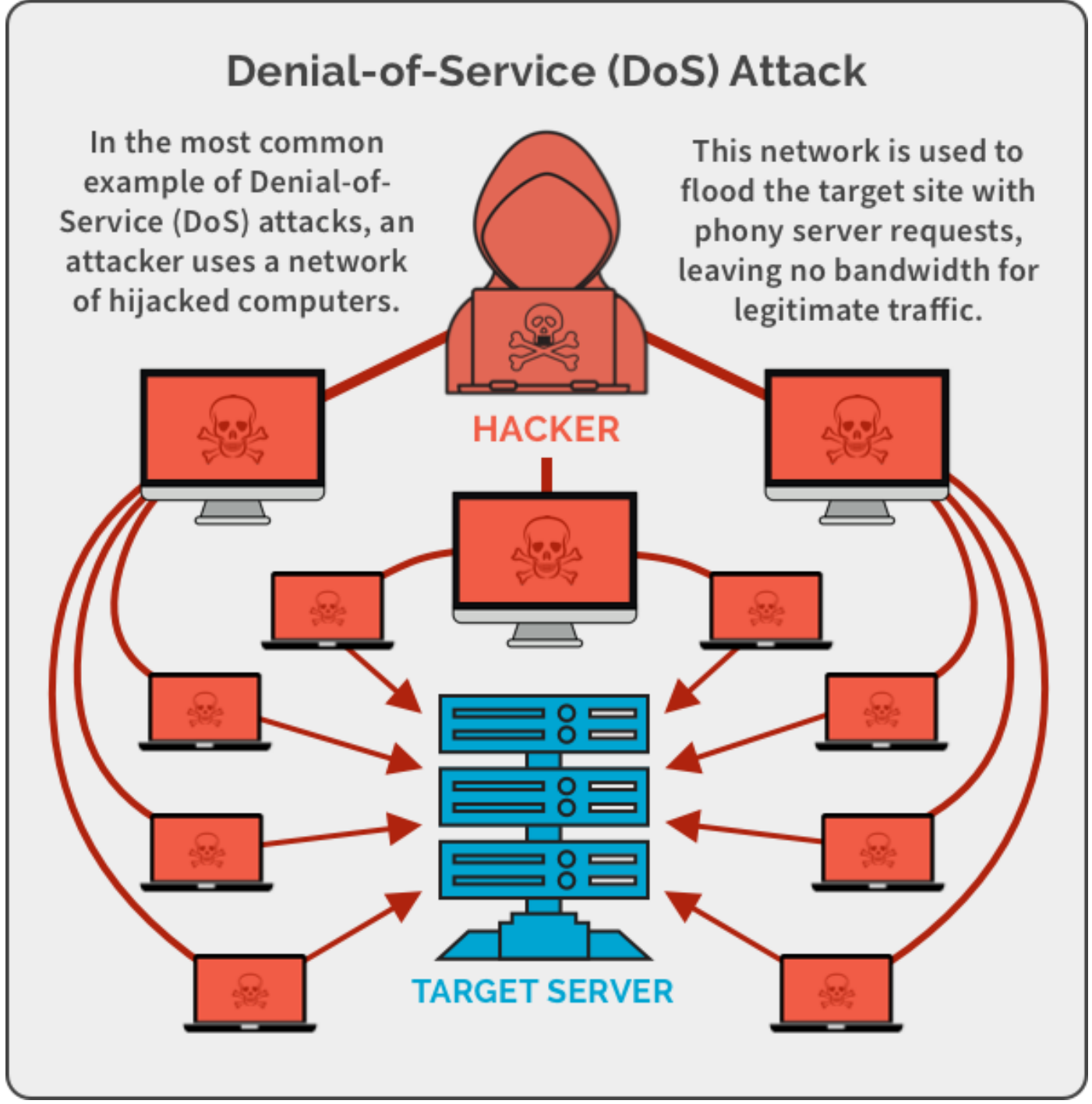
# How a Data Breach Occurs



# Threat and Mitigating Threats to IoT Systems

## Denial of Service (DoS) Attacks:

- **Threat: Attackers overload IoT devices or networks with a massive** volume of requests, causing service disruptions and rendering devices unresponsive.
- **Mitigation**: **Implementing traffic monitoring systems and anomaly detection mechanisms** can help identify and mitigate DoS attacks. **Network segmentation and load balancing** techniques can distribute and manage traffic effectively, minimizing the impact of such attacks.


Denial-of-Service (DoS) Attack
In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.
This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.
HACKER
TARGET SERVER

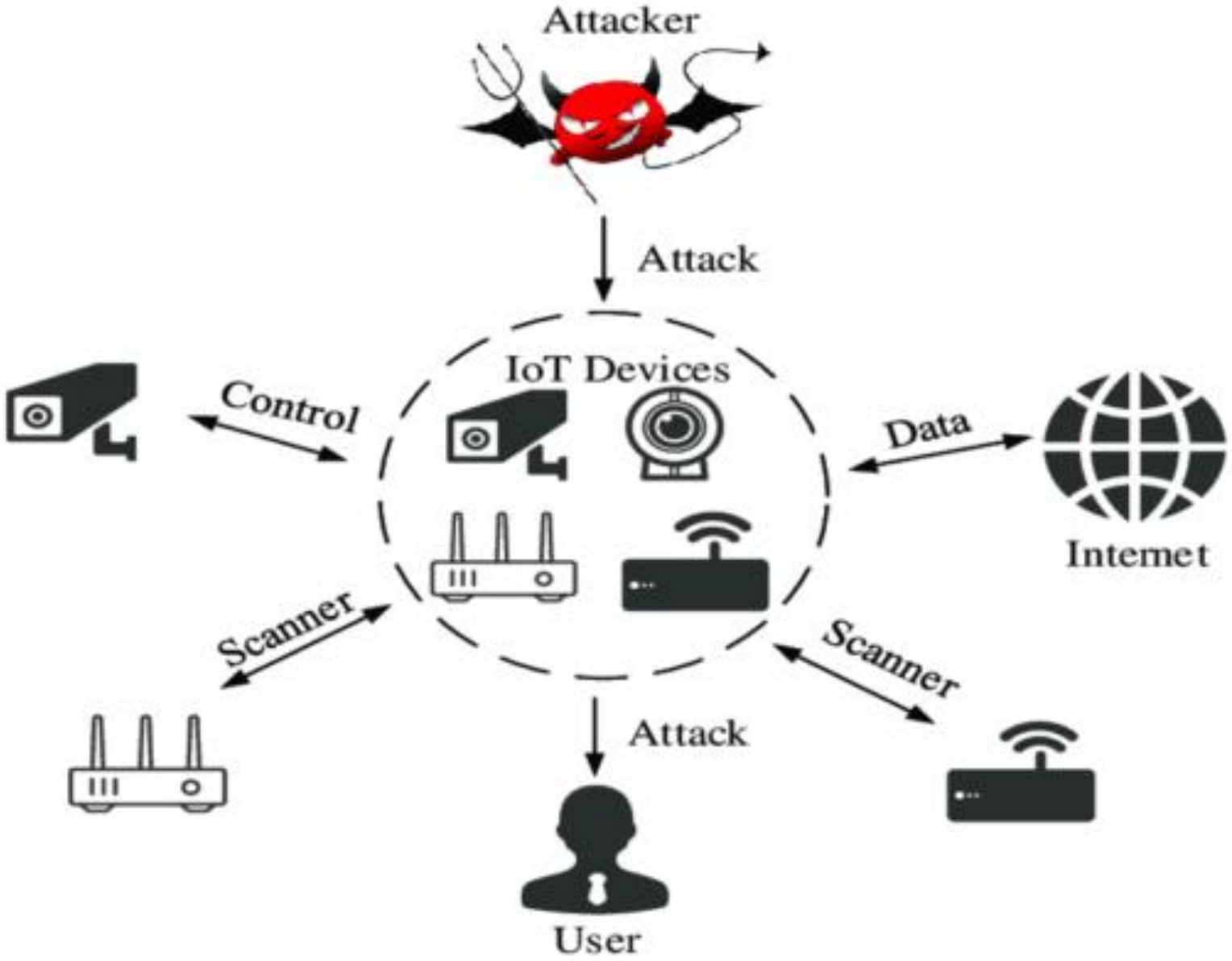
# Threat and Mitigating Threats to IoT Systems

## Physical Tampering:

- **Threat:** Physical tampering involves **attackers gaining physical access to IoT devices and manipulating them to compromise their security** or disrupt their functionality.

- **Mitigation: Physical security measures, such as tamper-evident seals, secure enclosures, or tamper detection sensors, should be employed to detect and deter physical tampering.** Encrypting stored data on devices can also protect sensitive information if the device falls into the wrong hands.

# Physical Tampering



# Threat and Mitigating Threats to IoT Systems

## Insecure Interactions:

- **Threat: Insecure communication channels and protocols can enable attackers** to intercept or manipulate data exchanged between IoT devices, **compromising the integrity and confidentiality** of the system.

- **Mitigation: Implementing secure communication protocols like HTTPS or MQTT** with appropriate encryption ensures that data transmitted between devices and backend systems remains secure. **Employing message authentication techniques, such as digital signatures or message integrity checks**, can prevent data tampering.

# Threat and Mitigating Threats to IoT Systems

## Insider Threats:

- **Threat: Insider threats involve malicious activities by individuals** with authorized access to IoT systems, such as employees or contractors, who exploit their privileges for personal gain or to cause harm.

- **Mitigation: Implementing access control mechanisms, least privilege principles, and robust identity and access management practices** can help minimize the risk of insider threats. **Regular monitoring of user activities and behavior analysis** can also aid in detecting and responding to suspicious activities.

# IOT Privacy concerns

- Privacy concerns in IoT refer to the **potential risks and threats to the confidentiality, integrity, and control of personal information** in interconnected devices and systems. **The extensive collection, processing, and sharing of data in IoT environments** can raise significant privacy challenges that need to be addressed to protect individuals' rights and maintain trust in IoT technologies.

- **Wearable Health Trackers: IoT-enabled wearable devices that monitor health and fitness data, such as heart rate, sleep patterns**, and location, can provide valuable insights into individuals' well-being. **However, the extensive collection of such sensitive personal health data raises concerns about the security and privacy** of this information, as it could be accessed or used without proper consent or safeguards.

# Access Control

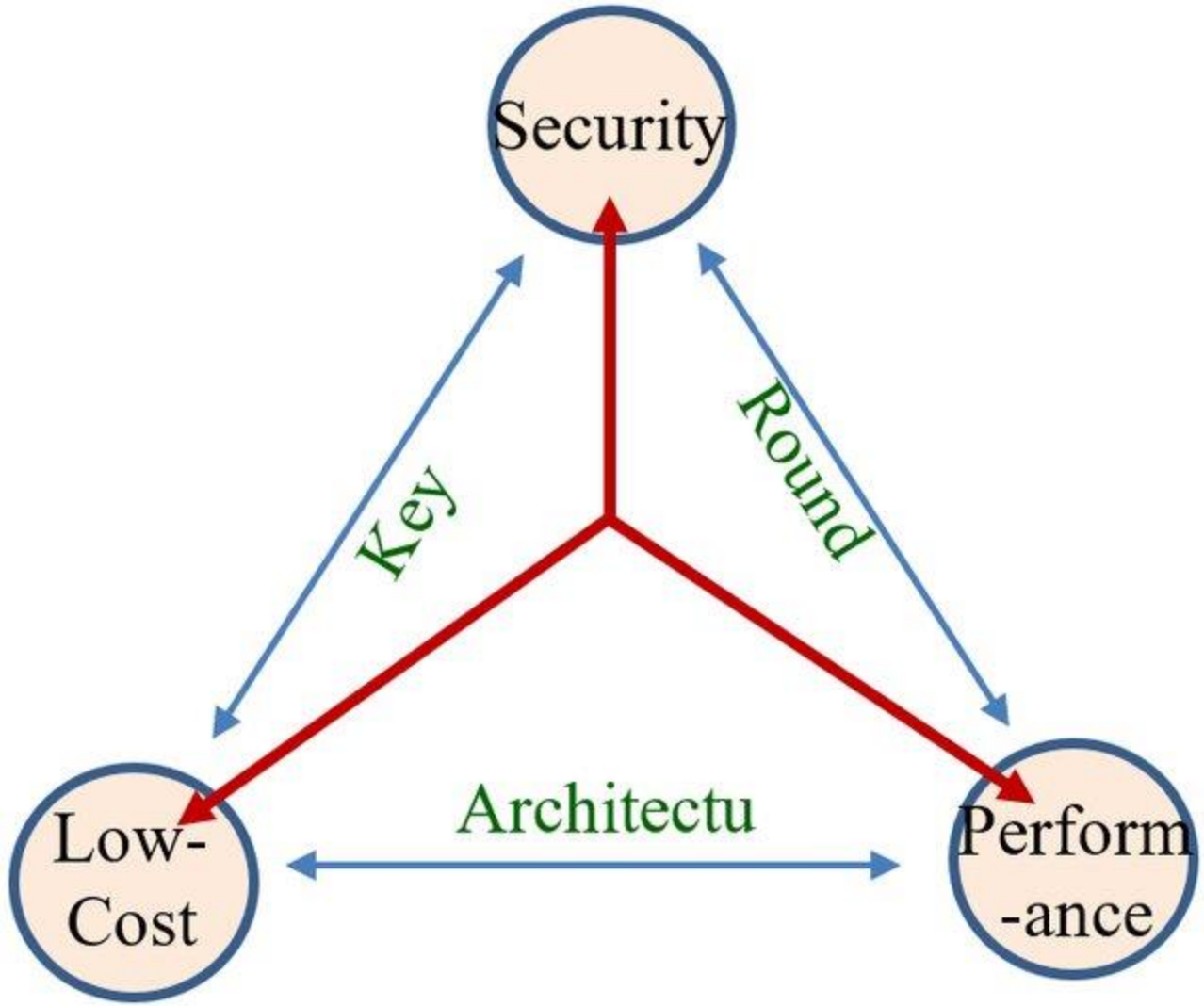
- **Access control** mechanisms play a crucial role in mitigating privacy risks and safeguarding user data in IoT systems.
- Access control is a **security technique** that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that **minimizes risk to the business or organization**.
- There are **two types** of access control: **physical and logical**. **Physical access control limits access to campuses, buildings, rooms and physical IT assets**. **Logical access control limits connections to computer networks, system files and data.**

# Access Control

- **To secure a facility**, organizations use **electronic access control systems that rely on user credentials**, **access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas**, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.
- **Logical access control systems perform identification authentication and authorization of users** and entities by evaluating required login credentials that can **include passwords, personal identification numbers, biometric scans, security tokens or other authentication factors**. **Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems.**

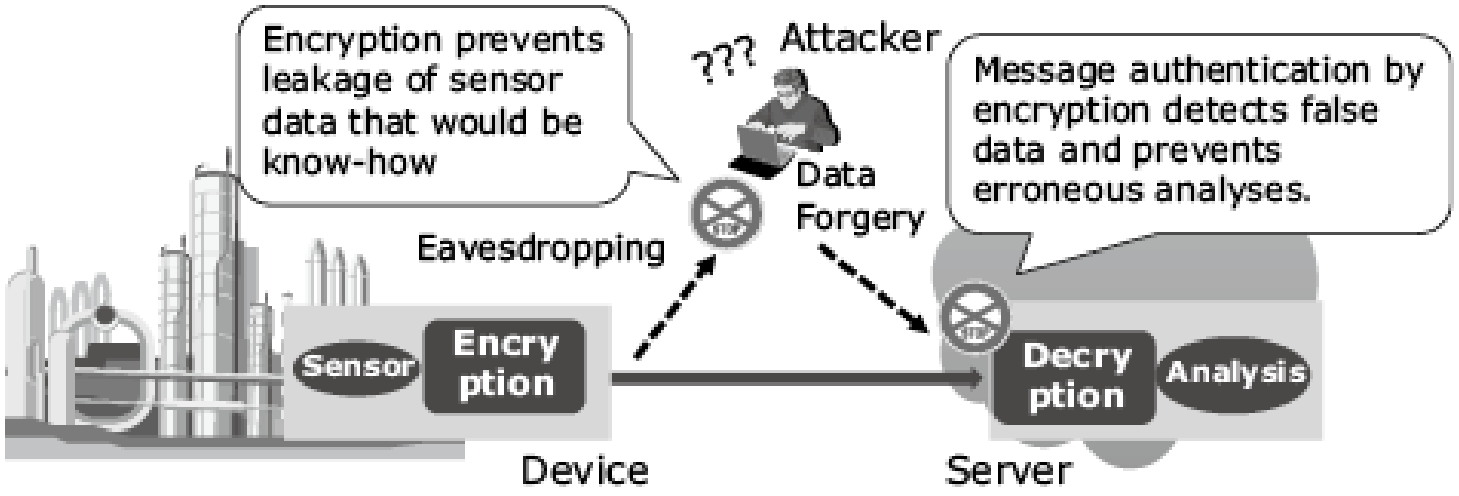
# Lightweight cryptography

- Lightweight cryptography is an **encryption method** that features a **small footprint and low computational complexity**.
- It refers to **cryptographic algorithms, protocols, and systems that are designed to be efficient, resource-friendly**, and suitable for **constrained environments like IoT devices**.
- The term **"lightweight"** emphasizes the goal of **minimizing computational, memory, and energy requirements** while still providing adequate security.
- It is designed to meet the requirements of **low-cost devices while still providing adequate security and performance**.
- These solutions aim to provide **robust security while minimizing the computational, memory, and power requirements of IoT devices**. **Privacy concerns in IoT can be addressed using lightweight cryptography** to protect sensitive data and ensure secure communication.


Security
Key
Round
Low-
Cost
Architectu
Perform
-ance

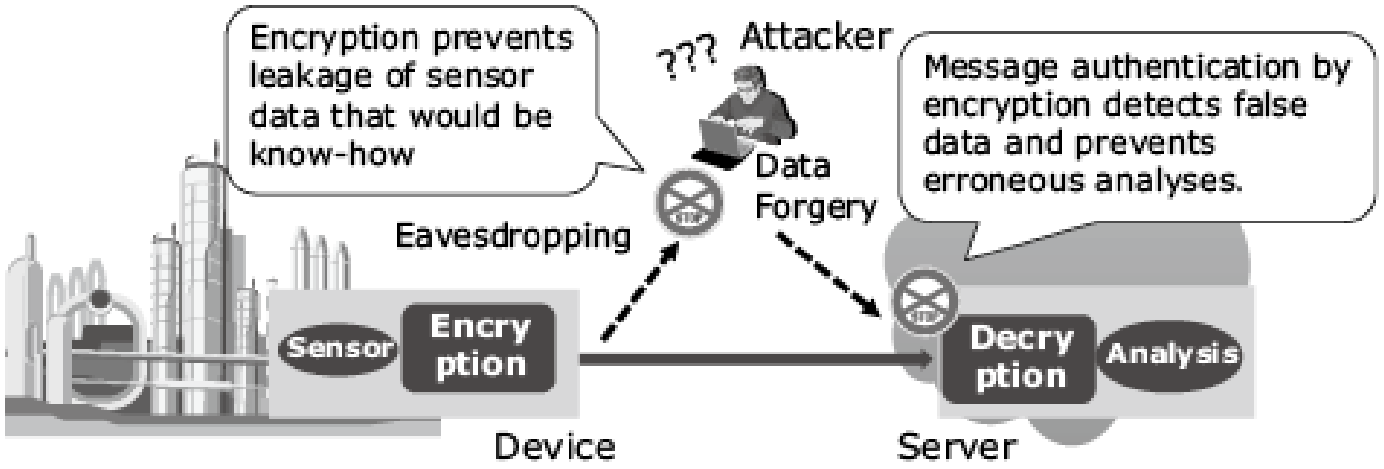
# Encryption-based counter measure against attack on data collection.

- Applying encryption to sensor devices means the **implementation of data protection for confidentiality and integrity**, which can be an effective **counter measure against the threats**.
- Lightweight cryptography has the function of enabling the application of **secure encryption, even for devices with limited resources.**



# Light Weight Cryptography

- The purpose of applying IoT to a plant is to significantly improve the productivity and maintainability by collecting data from a large number of sensors installed in production equipment, by analyzing it and performing autonomous control in real time.
- If sensor data should be falsified during this process, incorrect analysis results would be induced and erroneous control would result due to such an occurrence having the potential of leading to major damage.




- Moreover, since **measurement data and control commands are trade secrets** associated with the know-how of production and management, preventing leakages is also important from the **viewpoint of competitiveness.**
- Even if there is **no problem at present**, it is necessary to consider the effect of threats that might become evident in the future.

# Example of lightweight cryptography applications.

- **Smart Home:** The process begins with a temperature sensor measuring the **room's temperature,** which is then received by a **microprocessor**. The microprocessor performs necessary adjustments on the data and **encrypts it using a lightweight encryption algorithm**. The encrypted temperature data is then **transmitted via a communication module** and a **Wi-Fi connection, ensuring a secure connection to the internet**.
- **Through the internet, the encrypted data reaches a server processor for analysis**. At the server end, a **communication module receives the encrypted data** and passes it to the server processor, which is equipped with **decryption capabilities**. The server processor decrypts the data using the **same lightweight encryption algorithm**, allowing further analysis or control actions to be performed. By applying lightweight cryptography, the temperature data remains protected and confidential during transmission, preventing unauthorized access or tampering.