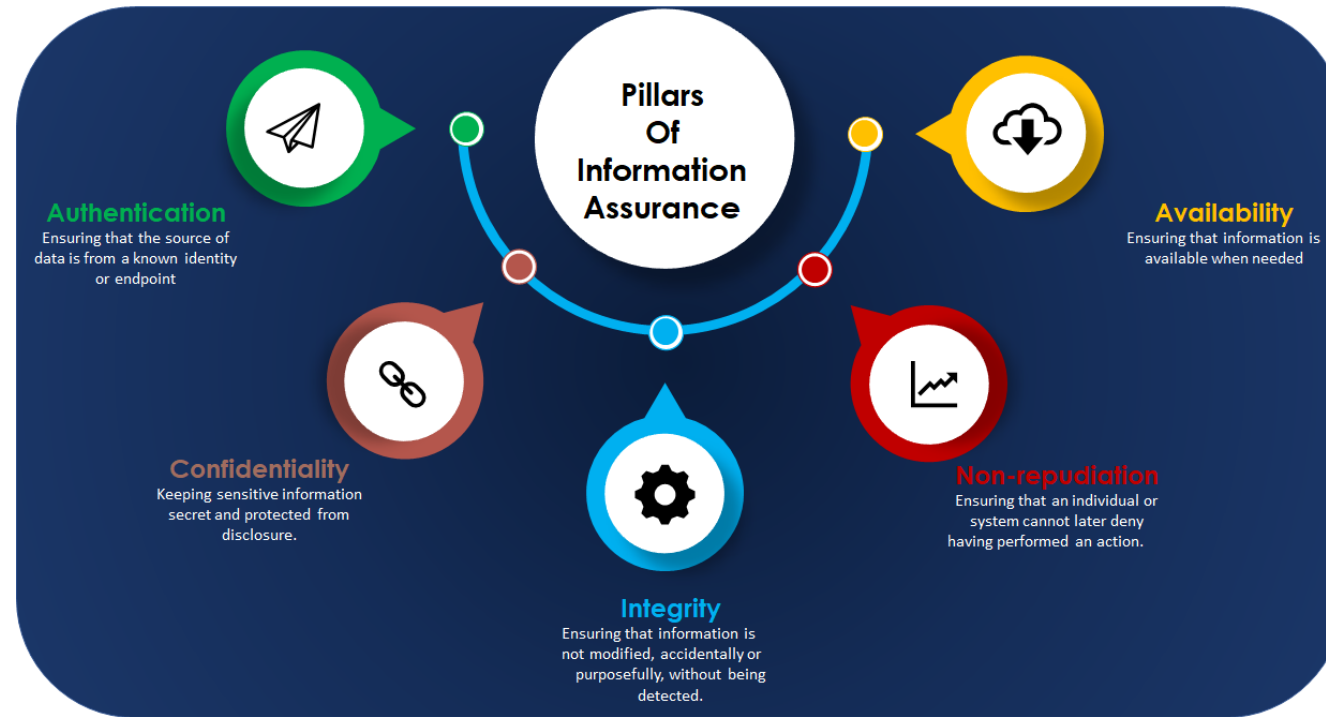


# CHAPTER 3

Internet of Things Security Requirements, Threats, Attacks, and  
Countermeasures





# SECURITY REQUIREMENTS IN INTERNET OF THINGS



# SECURITY REQUIREMENTS IN INTERNET OF THINGS



**IOT THREATS,  
ATTACKS,  
VULNERABILITIES,  
AND RISKS**

**IoT Threats**

**IoT Vulnerabilities**

**IoT Risks**

Features	Active Threats	Passive Threats
Modification	Modification in information takes place.	While in passive attack, Modification in the information does not take place.
Security target	Endanger the availability and Integrity.	Endanger for Confidentiality.
Community Focus	attention is on detection.	attention is on prevention.
The impact	system is always damaged.	There is not any harm to the system.
Victim awareness	A victim gets notified about the threats.	A victim does not get notified about the threats.
Resources	IoT resources can be changed.	IoT resources are not changing.
Services	They interrupt the services of the system.	Just acquire the information and messages in the system
Categories	<ul style="list-style-type: none"> <li>• Interruption threats</li> <li>• Modification threats</li> <li>• <u>Fabrication threats</u></li> </ul>	<ul style="list-style-type: none"> <li>• Traffic analysis</li> <li>• Release of message contents</li> <li>• Passive reconnaissance</li> </ul>

# IOT THREATS



# **TODAY'S IOT ATTACKS AND COUNTERMEASURES**

Physical IoT attacks

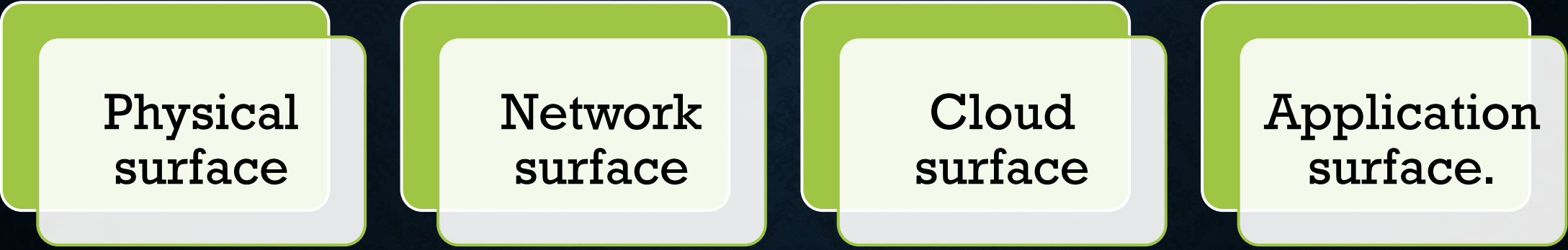
Software-related IoT attacks

Data-related IoT attacks

Protocol-related IoT attacks



# IOT ATTACK SURFACES



The diagram consists of four identical rectangular boxes arranged horizontally. Each box has a light green top half and a light gray bottom half, with a thin white border. The text is centered in the white area of each box.

Physical  
surface

Network  
surface

Cloud  
surface

Application  
surface.