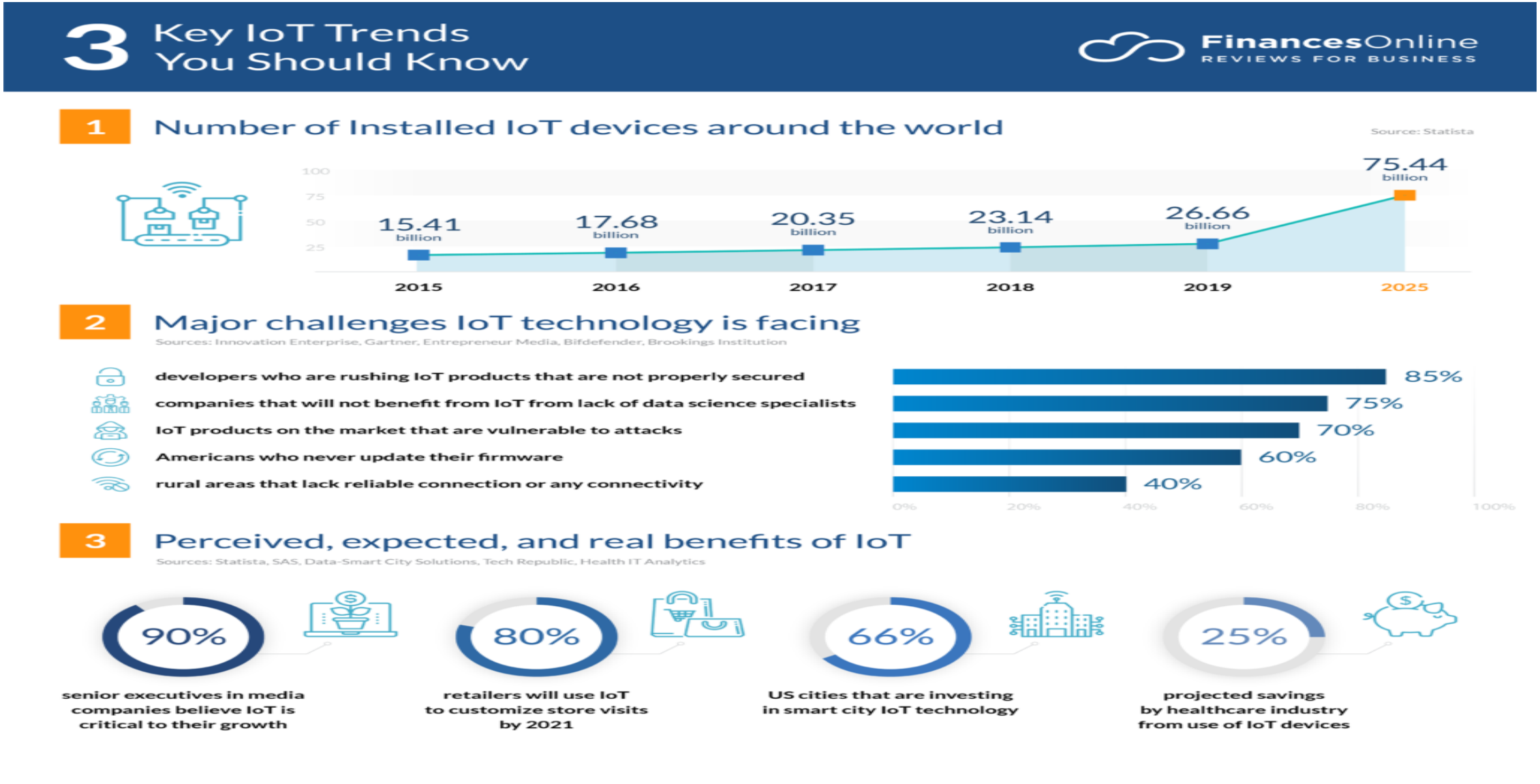
# IoT Security

Lec-1

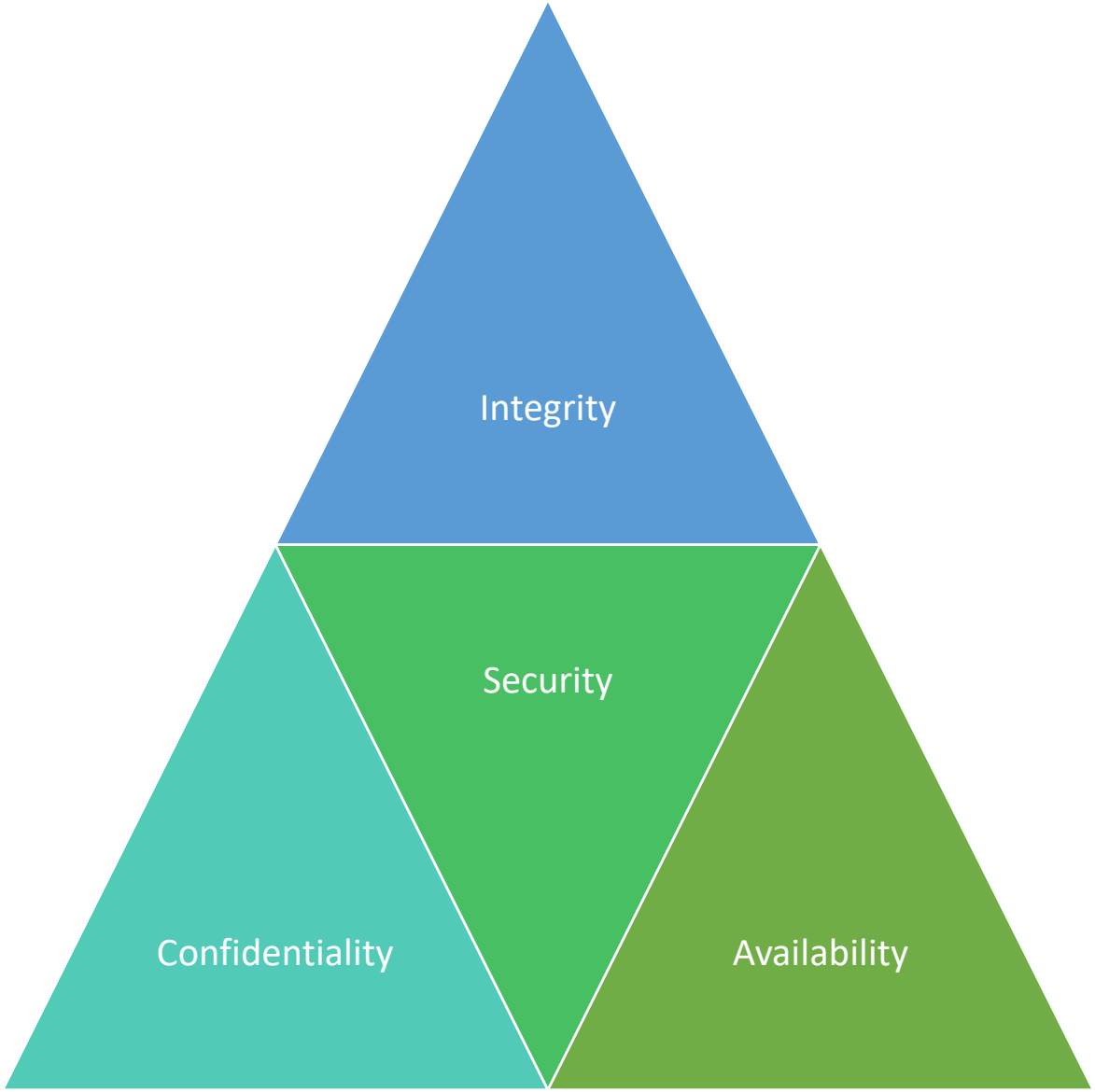
# Agenda

- Introduction to Security in IoT Devices
- IoT Trends
- Security Goals
- Security Services
- Security Mechanisms
- IoT Vulnerabilities
- Types of Attacks in IoT environment
- IoT attack Detection Mechanisms

# IoT Trends


3 Key IoT Trends You Should Know
FinancesOnline
REVIEWS FOR BUSINESS
1 Number of Installed IoT devices around the world
Source: Statista
100
75
50
25
15.41 billion
17.68 billion
20.35 billion
23.14 billion
26.66 billion
75.44 billion
2015
2016
2017
2018
2019
2025
2 Major challenges IoT technology is facing
Sources: Innovation Enterprise, Gartner, Entrepreneur Media, Bifdefender, Brookings Institution
developers who are rushing IoT products that are not properly secured
85%
companies that will not benefit from IoT from lack of data science specialists
75%
IoT products on the market that are vulnerable to attacks
70%
Americans who never update their firmware
60%
rural areas that lack reliable connection or any connectivity
40%
0%
20%
40%
60%
80%
100%
3 Perceived, expected, and real benefits of IoT
Sources: Statista, SAS, Data-Smart City Solutions, Tech Republic, Health IT Analytics
90%
senior executives in media companies believe IoT is critical to their growth
80%
retailers will use IoT to customize store visits by 2021
66%
US cities that are investing in smart city IoT technology
25%
projected savings by healthcare industry from use of IoT devices

# Security Goals



# Security Goals

- **Confidentiality:** Confidentiality means the protection of data or assets from the unauthorized access. It is applicable not only to the data stored in the system but also to the data in transmission eg. Hiding sensitive information in the military or the industry from competitors.
- **Integrity:** Protection of data from modification of any kind like insertion, deletion and replaying by the attacker i.e. only the authorized user can make changes to the data.
- **Availability:** It means that the information should be available to the user as and when he needs it. Data is of no use if it is not available on time.
- **Accountability**: The user is taking responsibility for his or her actions or it is possible to trace the actions to the system or user so that the responsibility for those actions can be established.

# Security Services

- **Data Confidentiality:** It is designed to protect data from disclosure attack. Aim is to protect data from traffic analysis and snooping.
- **Data Integrity:** It  is designed to protect data from unauthorized modification.
- **Authentication:** It helps in proving the authenticity of the user/party at the other end of the line. It can be done in two ways:-
  - **Peer Entity Authentication:** It Proves the authenticity of the two parties during connection establishment in connection oriented communication
  - **Data origin Authentication:** It Proves the authenticity of the source or origin of data in connectionless communication

# Security Services

- **Non-repudiation:** This service protects against the repudiation by either of the two parties involved in communication i.e sender and receiver. With the proof of origin, sender cannot deny sending and with the proof of delivery, receiver cannot deny the reception of data.
- **Access control:** Here the word access can involve reading, writing, modifying and executing programs and so on and the term access control means protecting the data from unauthorised access.

# Security Mechanisms

Security Mechanisms are used to provide security services. A security service may be provided by one or combination of more than one security mechanism. Various security mechanisms are:-

**Encipherment:** Encipherment means covering or hiding the data. It can be done using cryptography or steganography

**Data Integrity**: It means creating a short checkvalue from the given data using some specific process and appending that checkvalue to the message at the sender side. At the receiver side, receiver also calculates the checkvalue using received data and then compares it with the one received from the sender. If the two checkvalues are same then the data integrity is preserved.

**Digital Signature**: It is a means of verifying the data by the sender and receiver by signing it electronically

# Security Mechanisms

Security Mechanisms are used to provide security services. A security service may be provided by one or combination of more than one security mechanism. Various security mechanisms are:-

**Authentication Exchange:** In authentication exchange, the sender and the receiver exchanges some messages among themselves to prove their identities to each other

**Traffic Padding:** It involves adding some bogus data to the original data traffic to prevent adversary from accomplishing his task of gaining unauthorised access using traffic analysis.

**Routing Control:** It means to select and to change continuously the routes available between the two parties to prevent eavesdropping on a specific route.

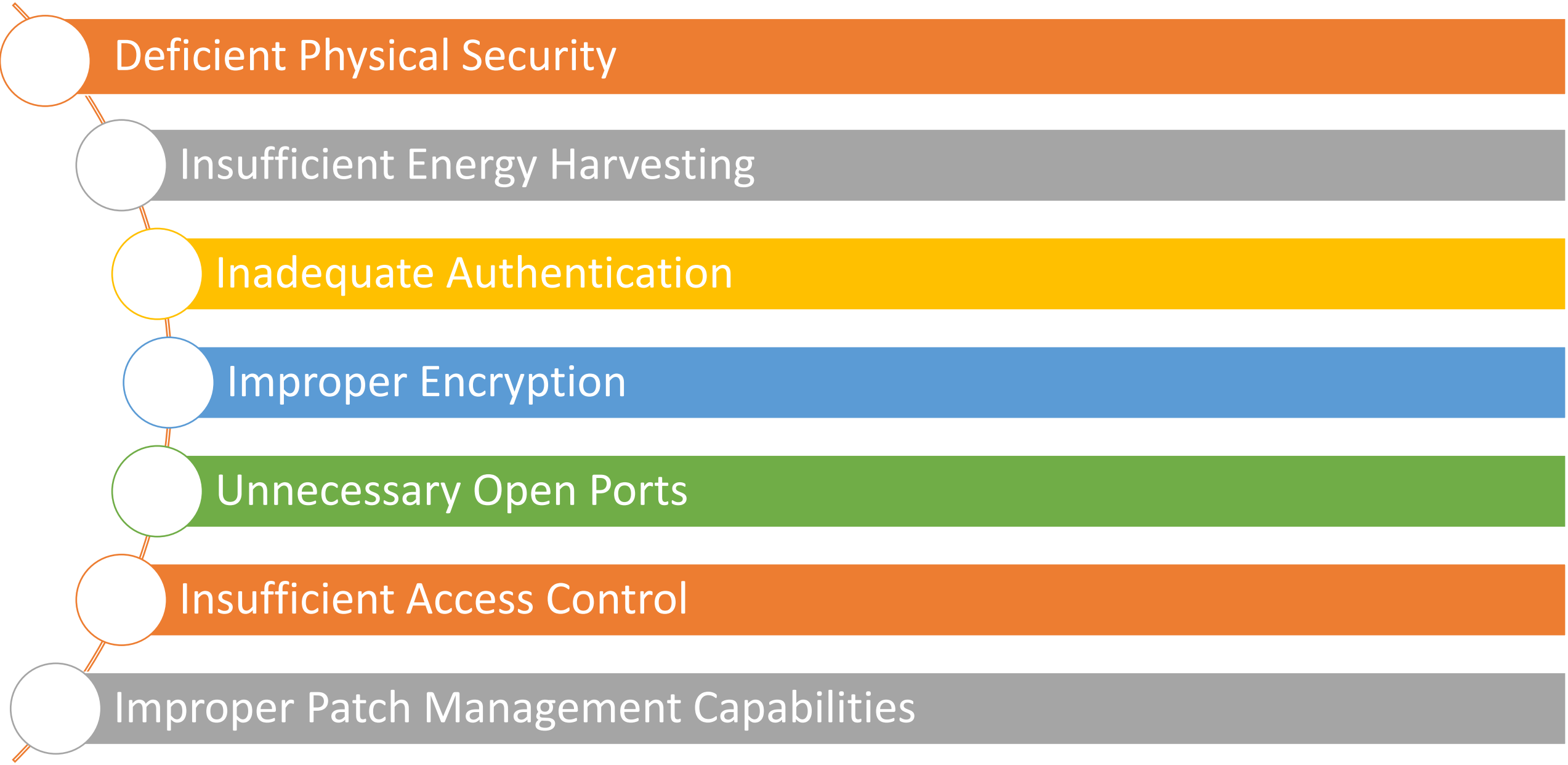
**Notarization:** It means appointing a third trusted party between the sender and the receiver to control the communication between them.

**Access Control:** It can use various methods to prove that the particular user has access to the particular data or resources. Some methods of proving access could be passwords or PINs.

# Vulnerabilities

- Vulnerability can be defined as the incompetency of the system which can be exploited by the attacker to attack the system security.

# Common Vulnerabilities



# Deficient Physical Security

- Since most of the IoT devices operate independently in an unattended environment, an adversary can very easily get physical access to the system and can take control over them

- **What attacker can do after gaining physical access to the system ?**
  - Physical Damage to the device.
  - Unveiling cryptographic scheme used
  - Gain root passwords
  - Modify boot parameters
  - Firmware Replication using malicious node

# Insufficient Energy Harvesting

- As IoT devices are characterized to have low energy and also no mechanism to renew it on their own.

➢**What an attacker can do?**

- Can  drain the battery of the device and make it unavailable to users.

# Inadequate Authentication

- Due to the presence of constraints such as low computational power and limited energy, IoT devices cannot implement complex authentication mechanism because of which it is quite easy for an attacker to attack such devices.

➢**What an attacker can do?**

- can append any spoofed malicious node.
- Authentication keys exchanged may be corrupted.

# Improper Encryption

- More complex the encryption algorithm, stronger will be the cryptosystem, but the fact that IoT systems have limited resources make the encryption algorithms less effective, less efficient and less robust.

➢**What an attacker can do?**

- can easily break the cryptosystem and can gain access to the sensitive data.

# Unnecessary Open Ports

- Many IoT devices while running vulnerable services may have unnecessary open ports

➢**What an attacker can do?**

- an attacker can connect through open ports and exploit lots of vulnerabilities.

# Insufficient Access Control

- A strong credential management system is required to protect data from unauthorised access. Most of the IoT devices in conjunction with their cloud management solutions do not use sufficiently complex passwords. Rather, most of the devices do not ask user to change the default user credentials after installation.

➢ **What an attacker can do?**

- an attacker can easily access the device

# Weak Programming Practices

- To minimize the attack vectors and to increase the functional capabilities of IoT devices, their operating system and the embedded firmware should be patched properly. But unfortunately most of the manufacturers do not recurrently maintain security patches.

➢ **What an attacker can do?**

➢ Can easily modify firmware

# Improper Patch Management Capabilities

- It has been reported by many researchers that various firmware are released with some vulnerabilities such as root users as main access point, backdoors and lack of secure socket layer usage.

➢**What an attacker can do?**

- Can easily modify firmware
- Can inject false data

# Insufficient Audit Mechanisms

- Since most of the IoT devices do not have thorough logging procedures, making it possible to hide IoT generated malicious activities.

➢ **What an attacker can do?**

- Various malicious activities of attacker may go un-noticed

# Types of Attacks Based on Security Goals

Any activity that threaten any security goal or that compromise the IoT device can be termed as an attack to IoT system. Attacks can be classified broadly on the basis of the security goal that they threaten:

- **Attack against confidentiality:** These types of attacks are mainly done to get unauthorized access to the data or any resource to perform further malicious actions.
- **Attack against integrity:** Attacker can make unauthorized modifications to the data
- **Attack against Availability:** attacker makes the system unavailable to the legitimate users.

# Another Way of Categorising Attacks

## Active Attacks

- may change the data or harm the system.
- threaten the integrity and availability
- are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.
- Cannot be prevented by using encipherment
- Eg. Firmware modification, False data injection

## Passive Attacks

- The attacker's goal is just to obtain information.
- does not modify data or harm the system.
- threaten confidentiality
- Difficult to detect
- can be prevented by encipherment of the data.
- eg. snooping and traffic analysis are passive attacks.

# Thank you