MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

Data Security and Privacy in IoT

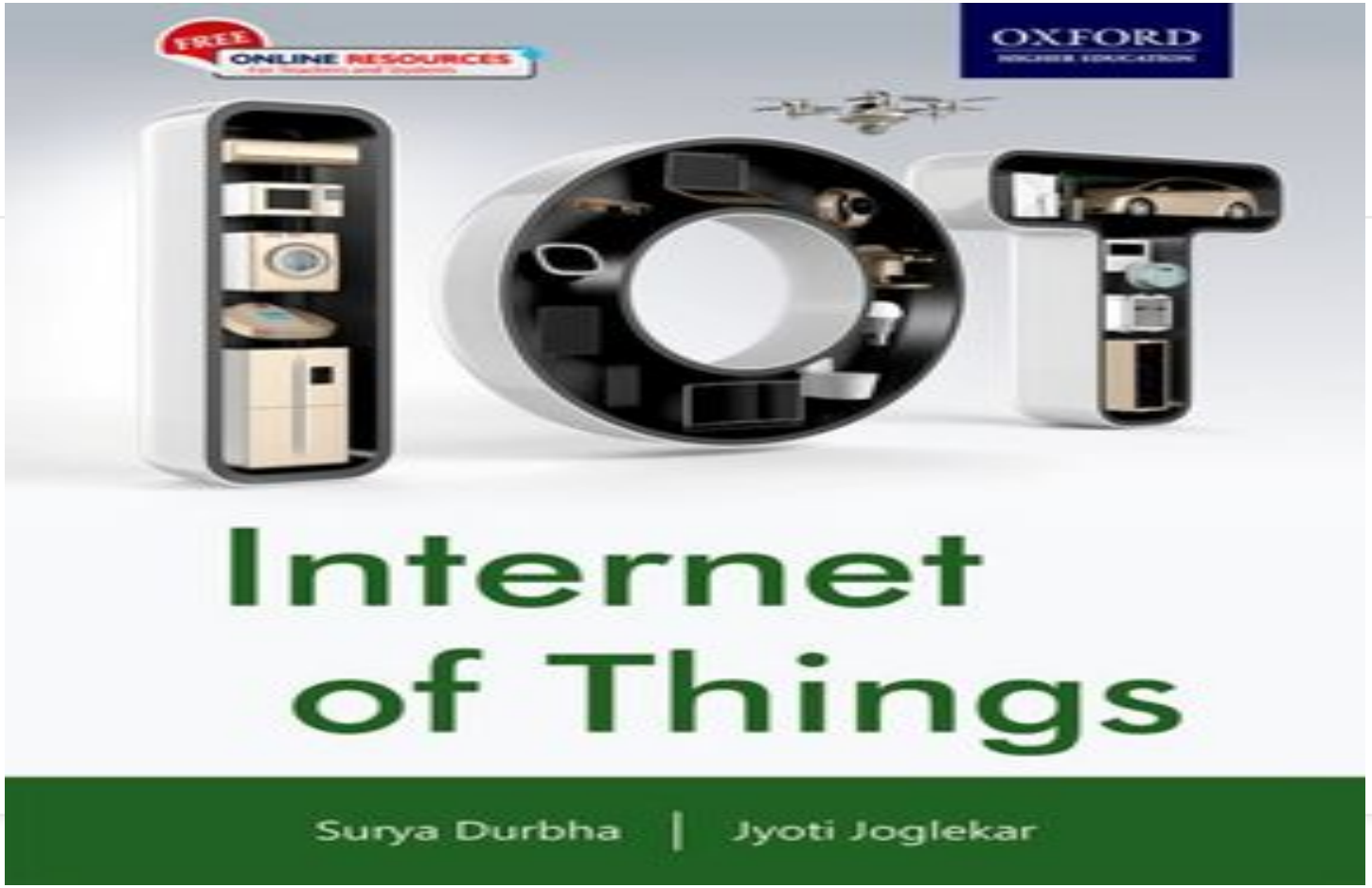
Agenda

- IoT Security Threats and Vulnerabilities
- Examples of Security Attacks
- Security Planning and Analysis
- Data Privacy and Ethical consideration in Data Management
- Case Study Analysis (Risk assessment &Threat Modelling Steps)

MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship



Recommended Book

https://www.amazon.in/Internet-Things-Surya-Durbha/dp/0190121092/ref=cm_cr_arp_d_bdcrb_top?ie=UTF8

MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

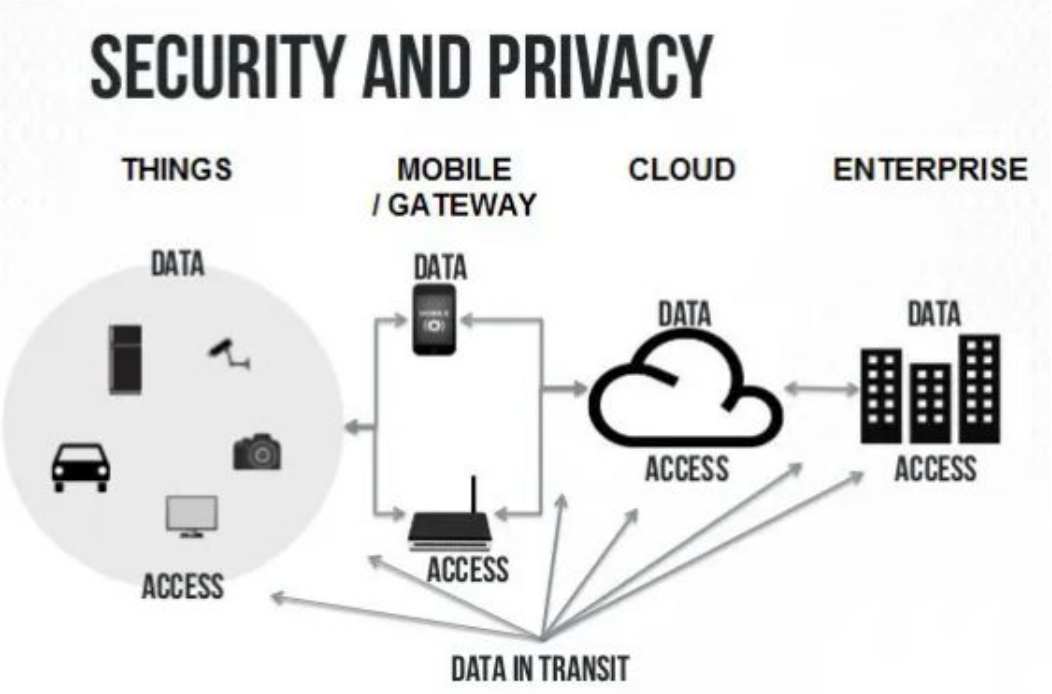
FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

IOT SECURITY THREATS AND VULNERABILITIES

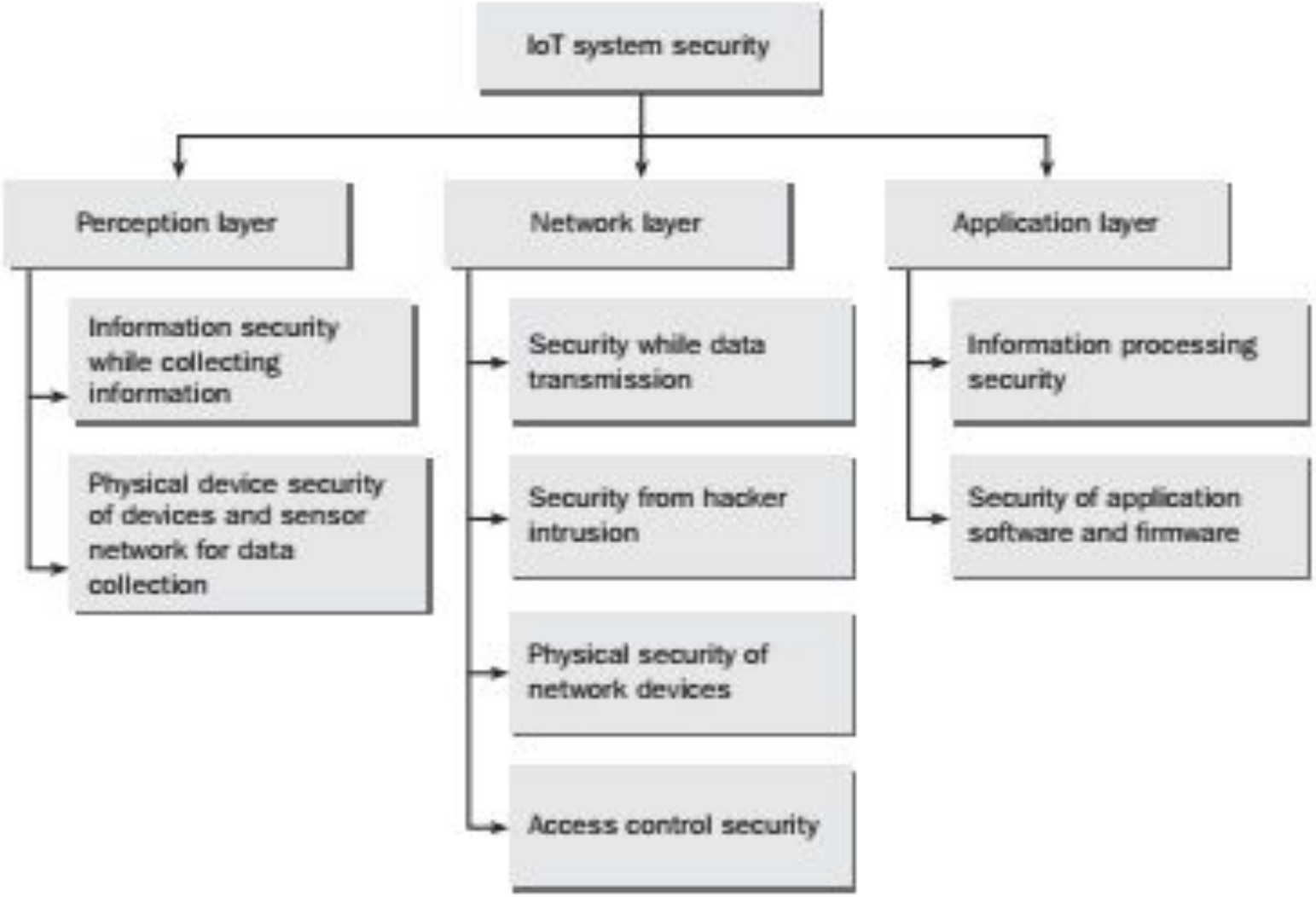
Introduction

Internet of Things (IoT) devices have become increasingly prevalent in various domains, ranging from smart homes and healthcare to industrial systems. However, the widespread adoption of IoT also brings about various security threats and vulnerabilities



Source : https://medium.com/@arindey/internet-of-things-iot-security-privacy-applications-trends-3708953c6200

In addition to data security, to develop a reliable application suitable for any business process, which is protected from all kinds of threats (e.g., interruption, interception, modification, and fabrication.

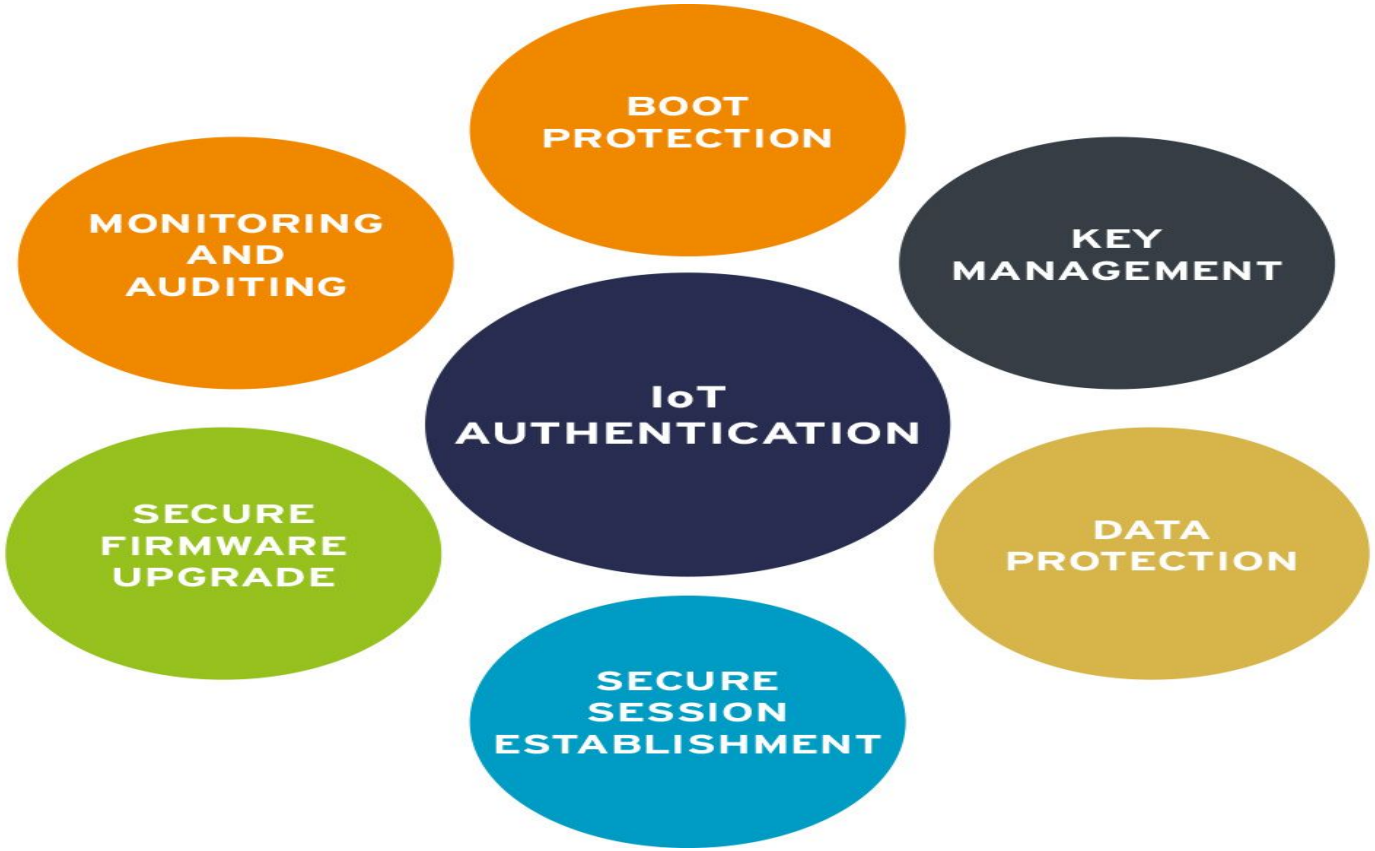


Source: Joglekar, Jyoti; Durbha, Surya. Internet Of Things (p. 331). Kindle Edition.

Inadequate Authentication and Authorization:

- Issue: Weak or hardcoded credentials, lack of proper authentication mechanisms, and insufficient authorization processes can lead to unauthorized access.
- Mitigation: Implement strong, unique passwords, use multi-factor authentication, and ensure proper authorization mechanisms are in place.

Device Authentication and Identity of Things (IDoT)



Lack of a common operating framework and security principles pose some serious challenges for device manufacturers and also the consumers.

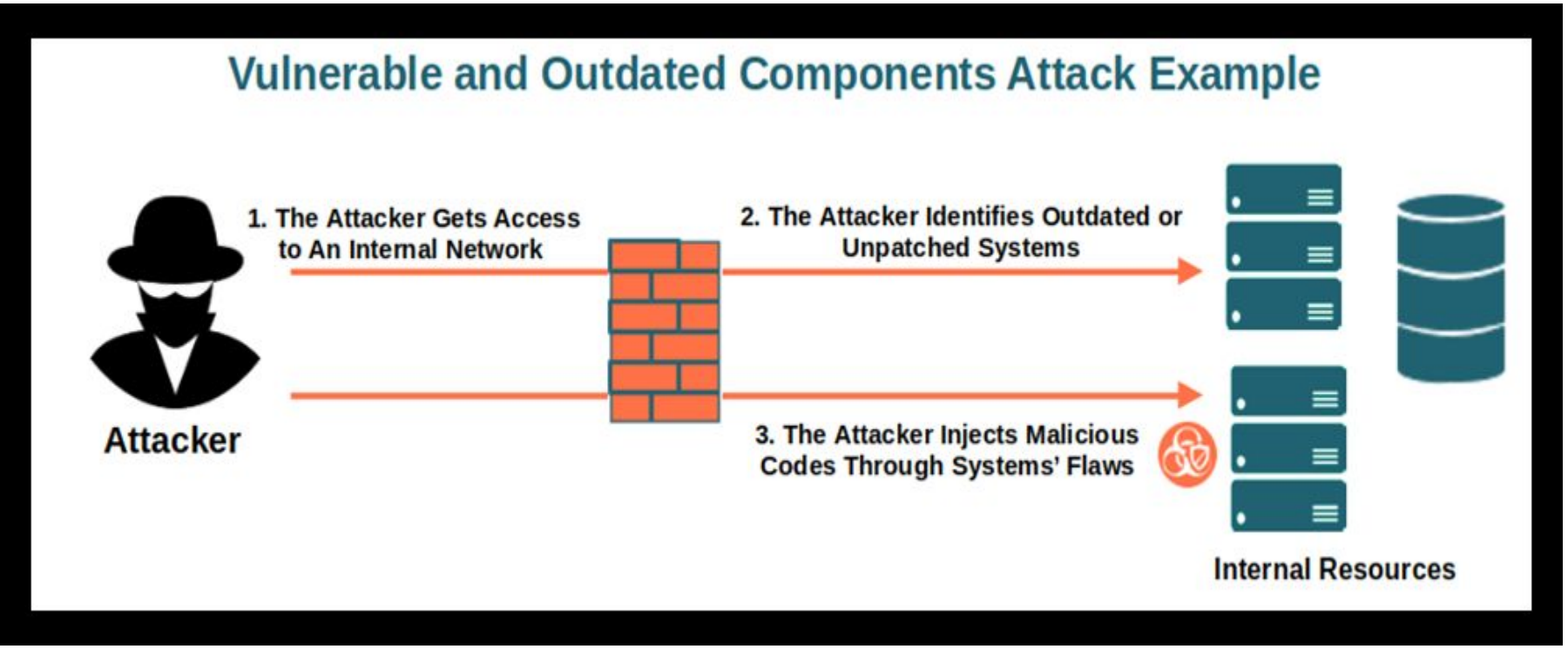
Source : https://www.kuppingercole.com/blog/singh/device-authentication-and-idot-for-iot

Lack of Encryption:

- Issue: Data transmitted between IoT devices and servers may be susceptible to interception, exposing sensitive information.
- Mitigation: Employ end-to-end encryption to secure data in transit and use encryption for data storage on devices.

Source :https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security

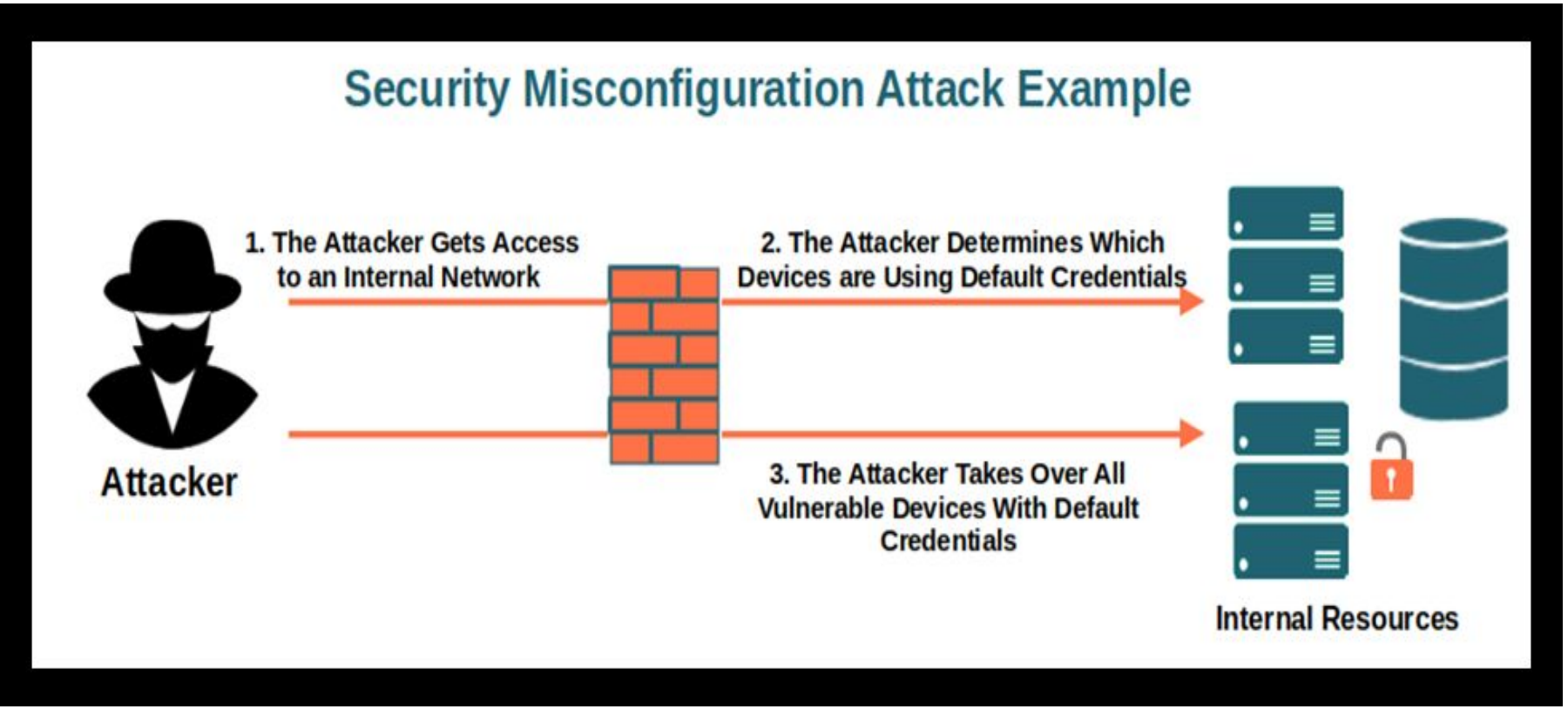
Insecure Device Firmware:



- Issue: Outdated or unpatched firmware may contain known vulnerabilities that attackers can exploit.
- Mitigation: Regularly update and patch device firmware, and ensure a secure update process is in place.

Source: https://cheapsslsecurity.com/blog/what-are-the-owasp-top-10

Insecure Network:



Source : https://cheapsslsecurity.com/blog/what-are-the-owasp-top-10-

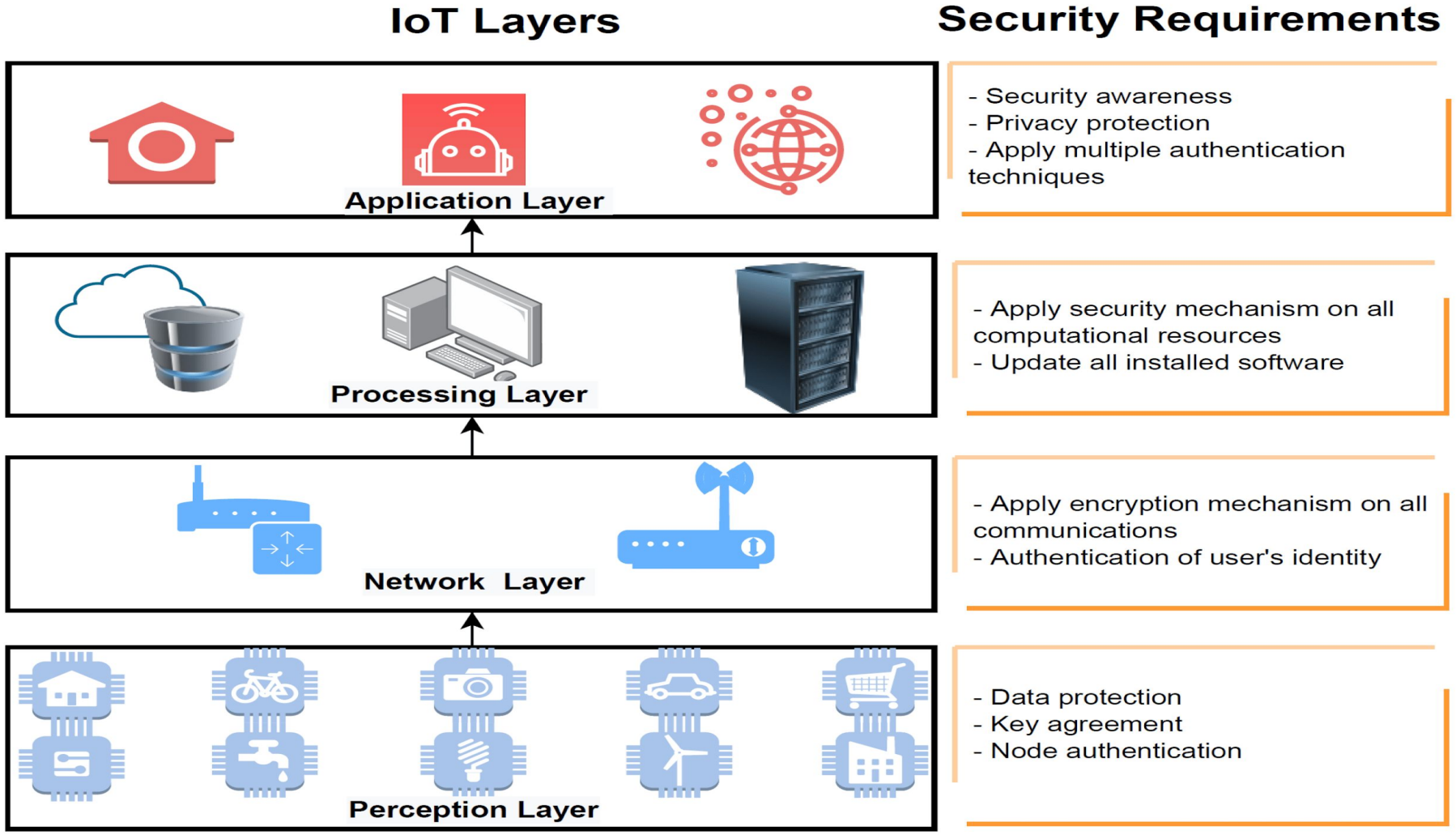
- Issue: Weaknesses in the network infrastructure, including unsecured Wi-Fi connections and unencrypted communication, can compromise IoT devices.
- Mitigation: Use secure network protocols, segment IoT devices from critical systems, and implement network security measures.

Physical Tampering:

- Issue: Physical access to IoT devices may lead to tampering, data extraction, or the installation of malicious hardware.
- Mitigation: Implement physical security measures, such as tamper-evident seals, and monitor devices for signs of tampering.

Source : https://community.arm.com/arm-community-blogs/b/internet-of-things-blog/posts/the-role-of-physical-security-in-iot

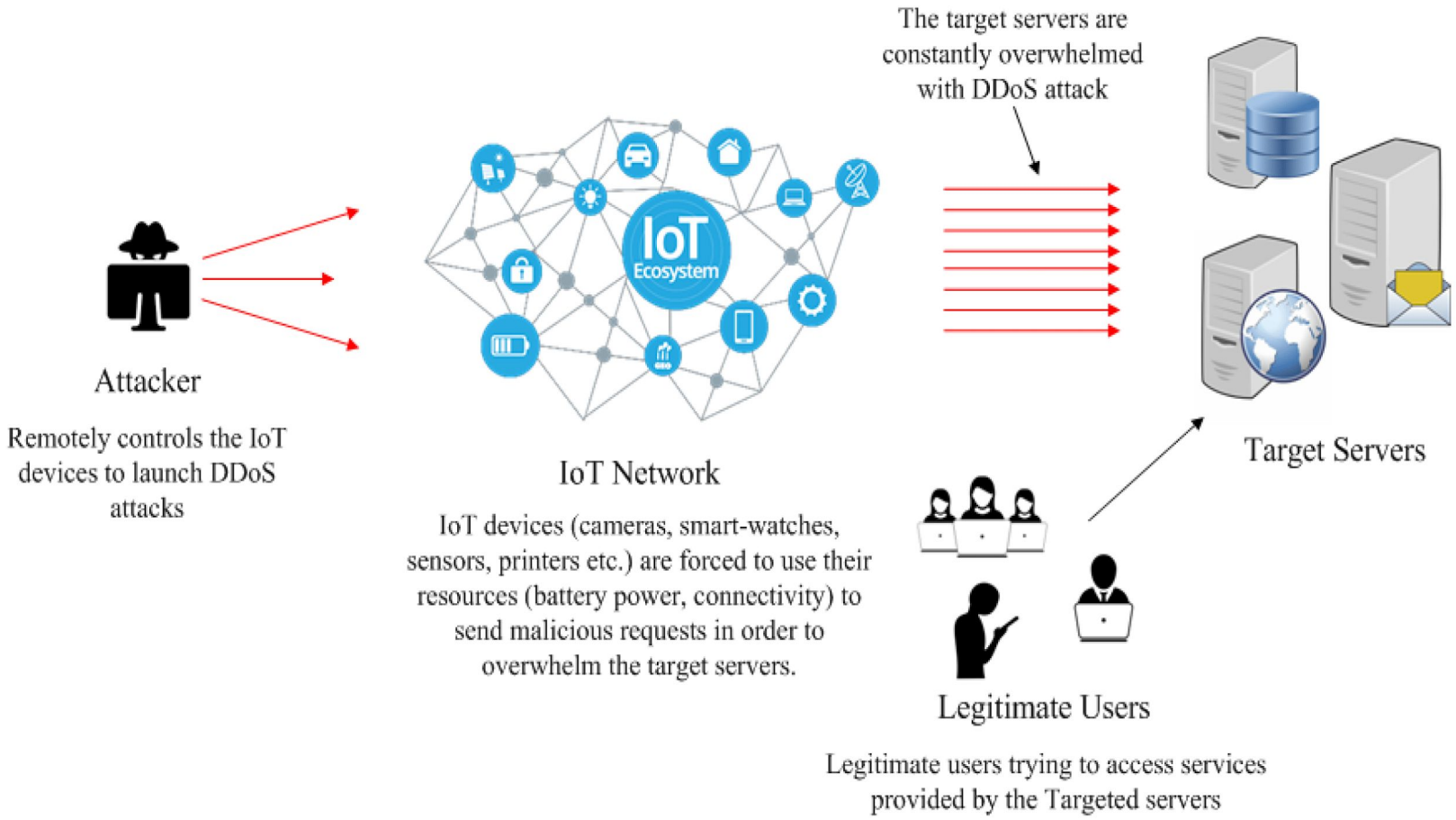
Insufficient Software Security:



Source: https://www.mdpi.com/2079-9292/10/7/848

- Issue: Insecure software design, coding practices, and lack of secure coding standards can result in exploitable vulnerabilities.
- Mitigation: Follow secure coding practices, conduct regular security audits, and use automated tools to identify and fix vulnerabilities.

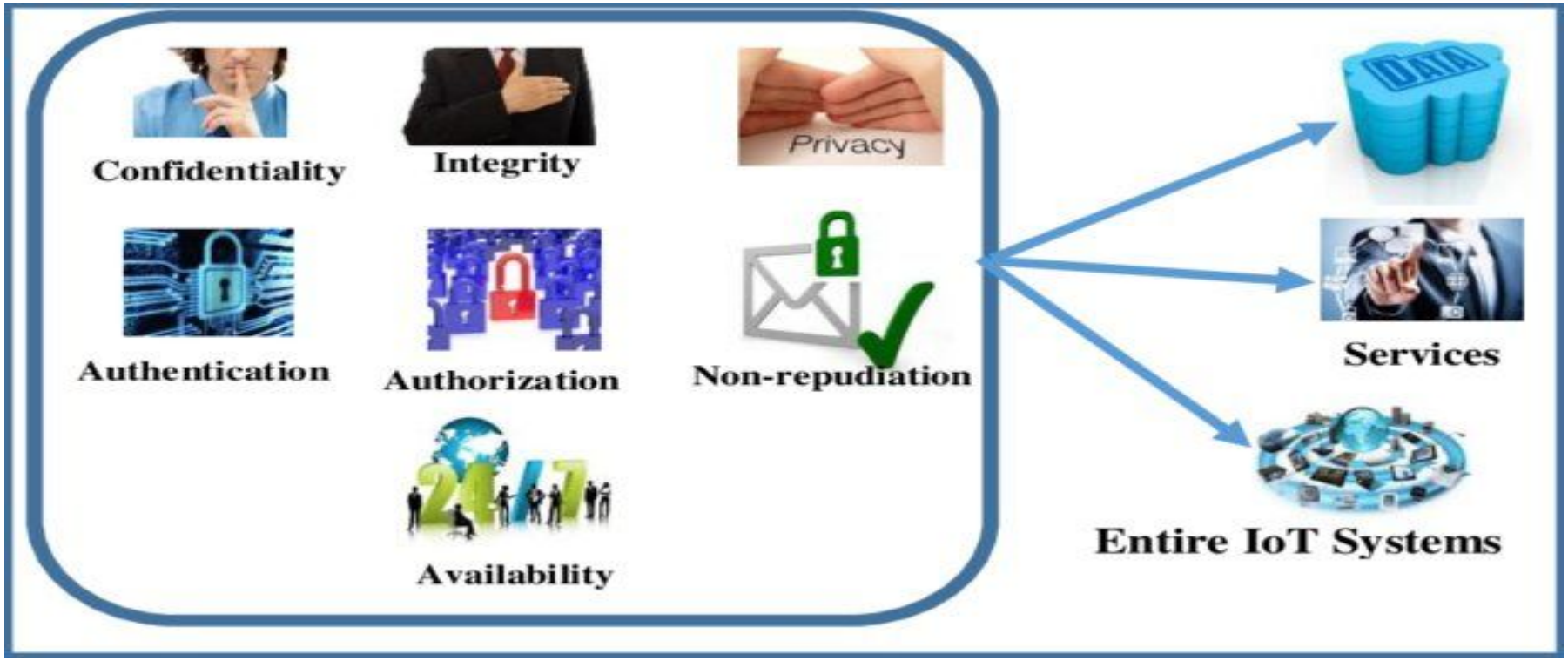
Denial of Service (DoS) Attacks:



- Issue: Attackers may flood IoT devices or networks with traffic, causing disruptions and making devices unavailable.
- Mitigation: Implement measures such as rate limiting, traffic filtering, and redundancy to mitigate the impact of DoS attacks.

Source: https://www.mdpi.com/1424-8220/22/3/1094

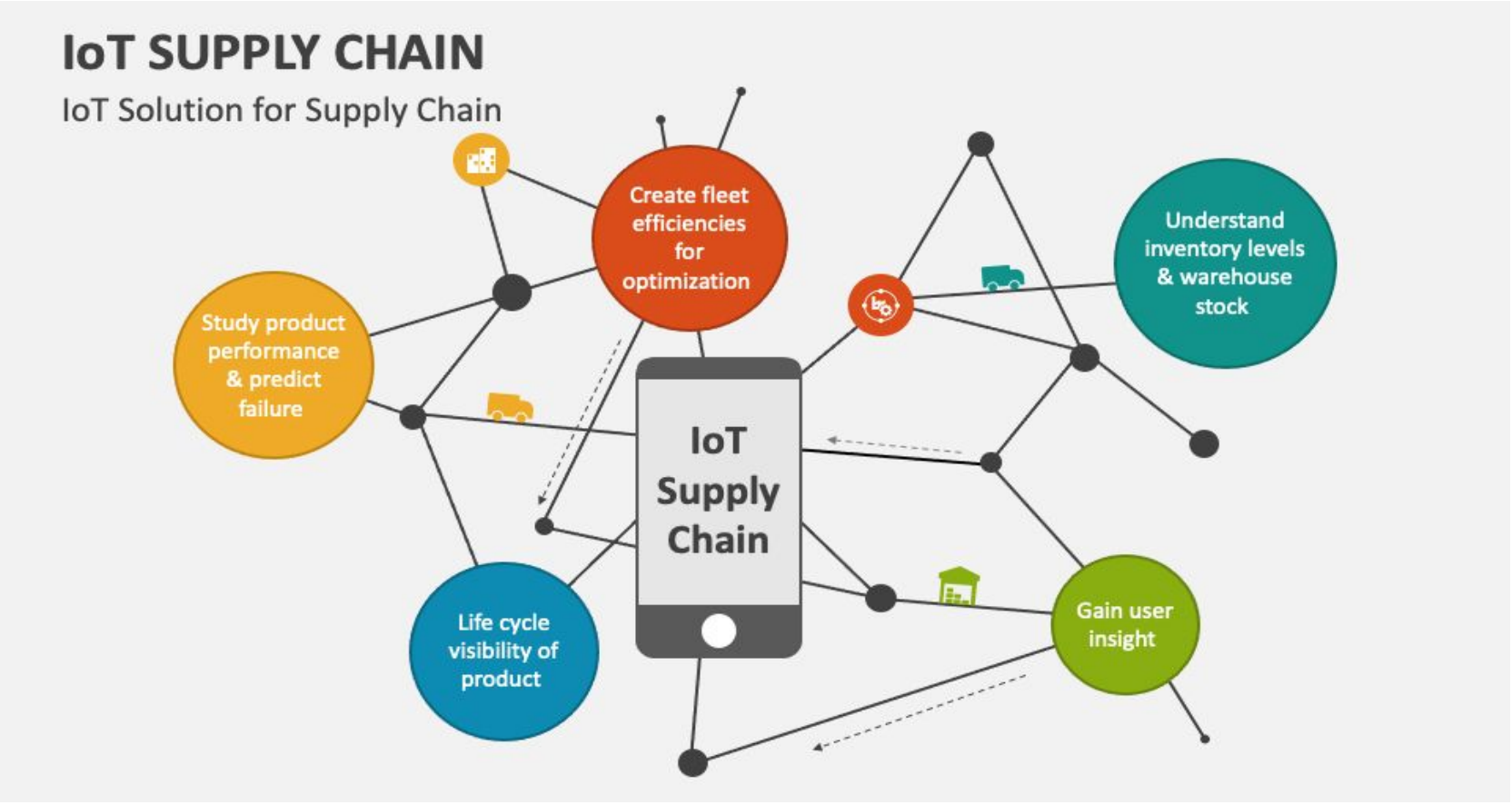
Privacy Concerns:



- Issue: Improper handling of user data and inadequate privacy policies can lead to unauthorized data access and privacy breaches.
- Mitigation: Clearly communicate privacy policies, anonymize or pseudonymize data when possible, and comply with relevant data protection regulations.

Source:https://www.researchgate.net/publication/308648065_Security_in_IoT_

Supply Chain Risks:

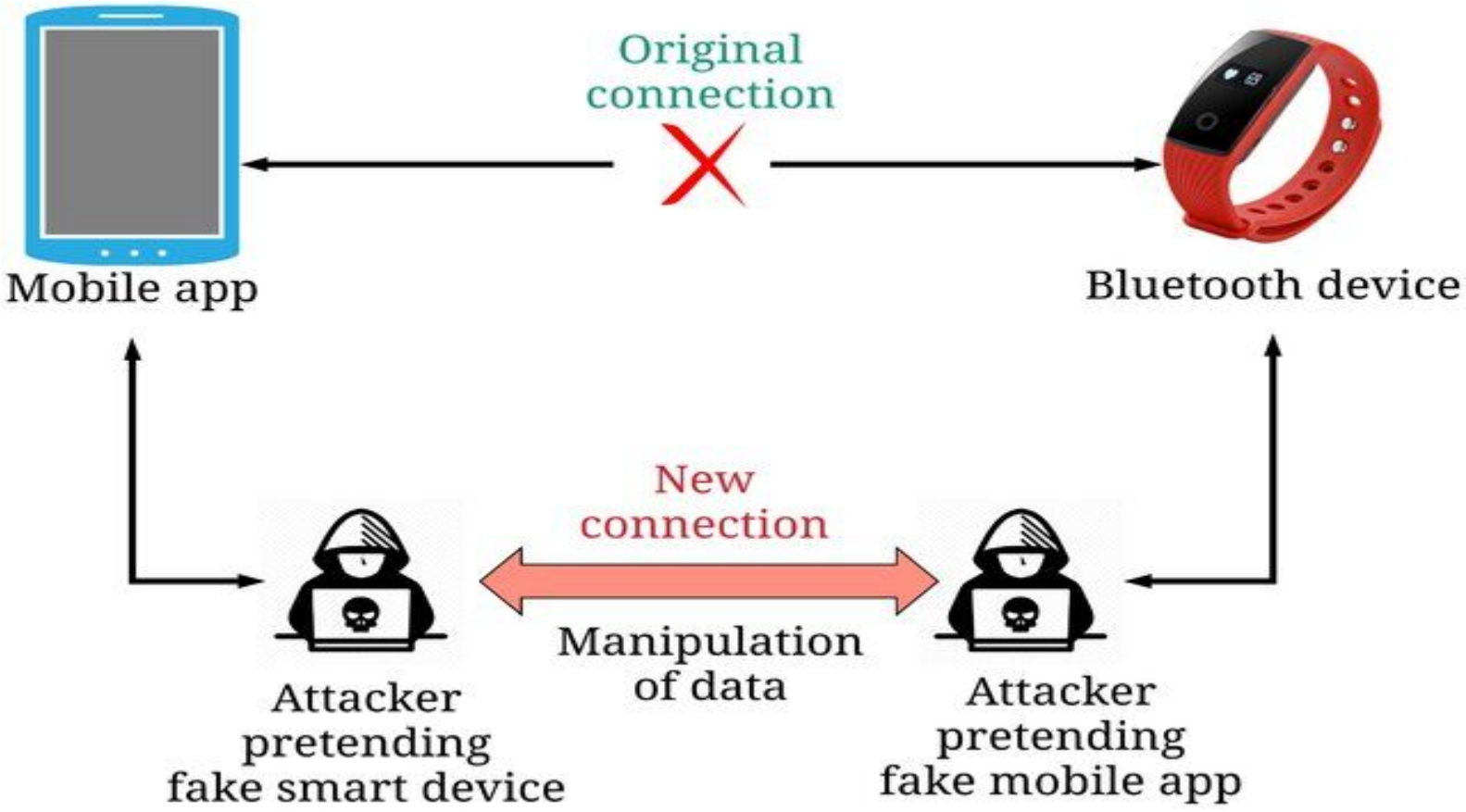


- Issue: Compromised components or malicious software introduced during the manufacturing process can pose significant risks.
- Mitigation: Implement a secure supply chain, conduct thorough vetting of suppliers, and validate the integrity of components.

Source: https://www.collidu.com/presentation-iot-supply-chain

Examples of security attacks

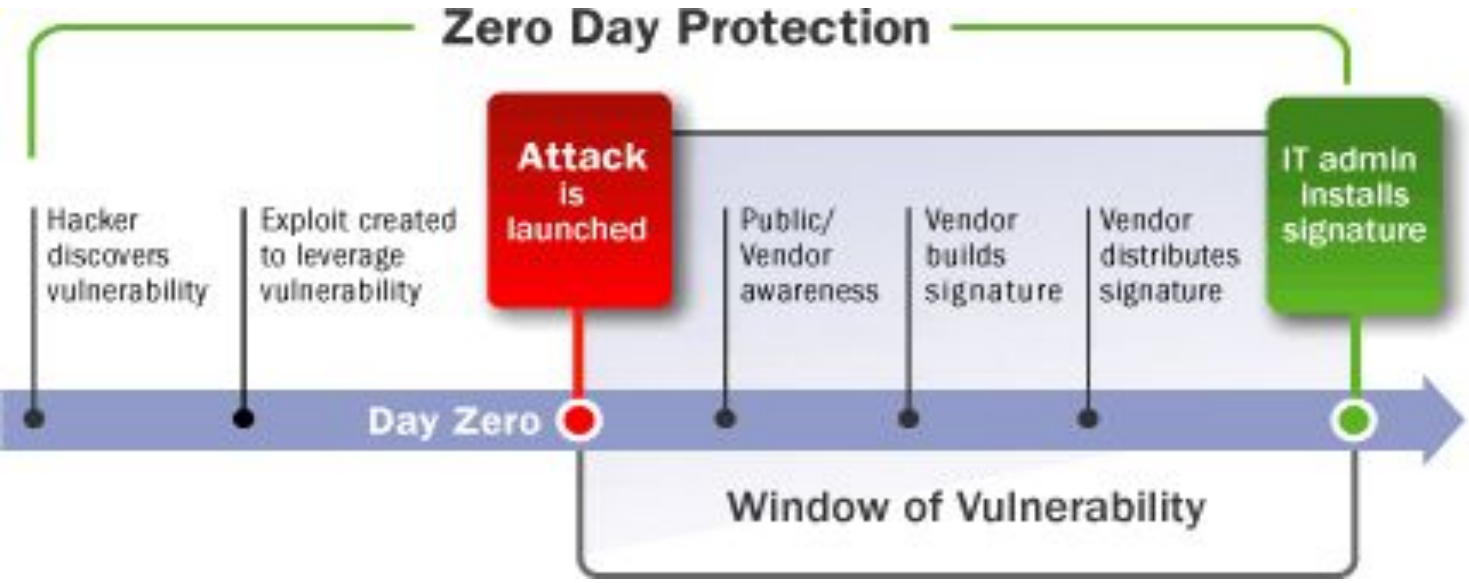
Man-in-the-Middle (MitM) Attacks:



- MitM attacks involve intercepting and potentially altering communication between two parties without their knowledge.
- Attackers can eavesdrop on sensitive information or manipulate data during transmission.
- This type of attack poses a significant threat to the confidentiality and integrity of communication channels.

Source:https://www.researchgate.net/publication/358416762

Zero-Day Exploits:



- Zero-Day Exploits target undisclosed vulnerabilities in software or hardware systems before a patch or fix is available.
- Attackers exploit these vulnerabilities to compromise systems, as there is no defense or mitigation in place.
- The term "zero-day" refers to the fact that developers have had zero days to address and rectify the issue.
- Organizations need to stay vigilant and apply security patches promptly to mitigate the risk of zero-day exploits.

Source :https://www.embedded.com/mitigating-zero-day-threats/

MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

Security planning and analysis

Why Plan for Security:

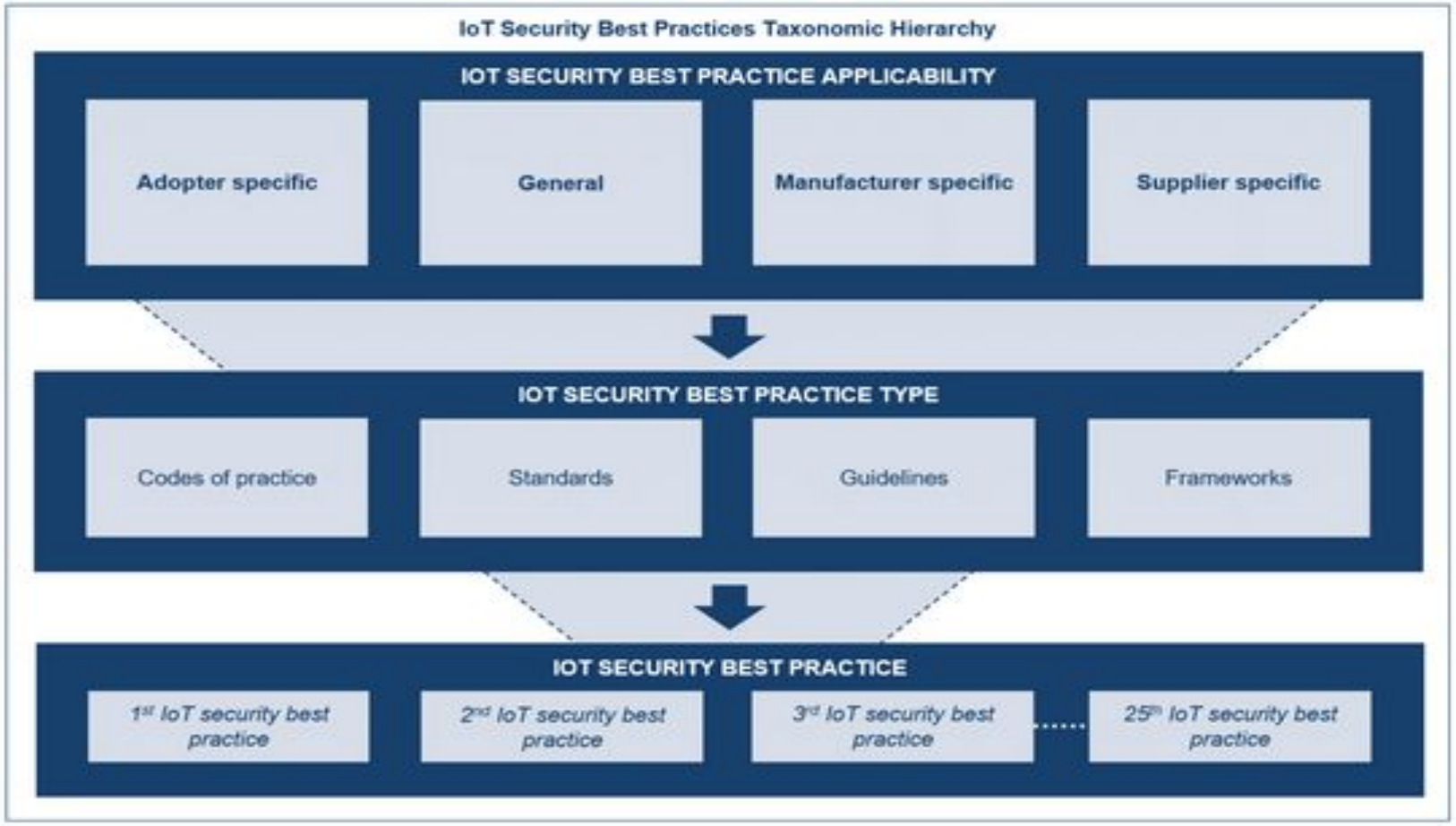
- Security planning in IoT is like creating a roadmap to keep our smart devices safe.
- It's essential because, just like with any journey, having a plan helps us avoid potential problems along the way.
- In the world of IoT, security planning is a proactive approach to prevent issues before they happen.

Components of Security Planning:

- It involves breaking down the plan into key components.
- These include things like risk assessment, which helps us identify potential problems, device authentication to make sure only authorized devices can access our network, and encryption to keep our data safe from prying eyes

Source : Joglekar, Jyoti; Durbha, Surya. Internet Of Things (p. 333). Kindle Edition.

Identifying and Prioritizing Risks

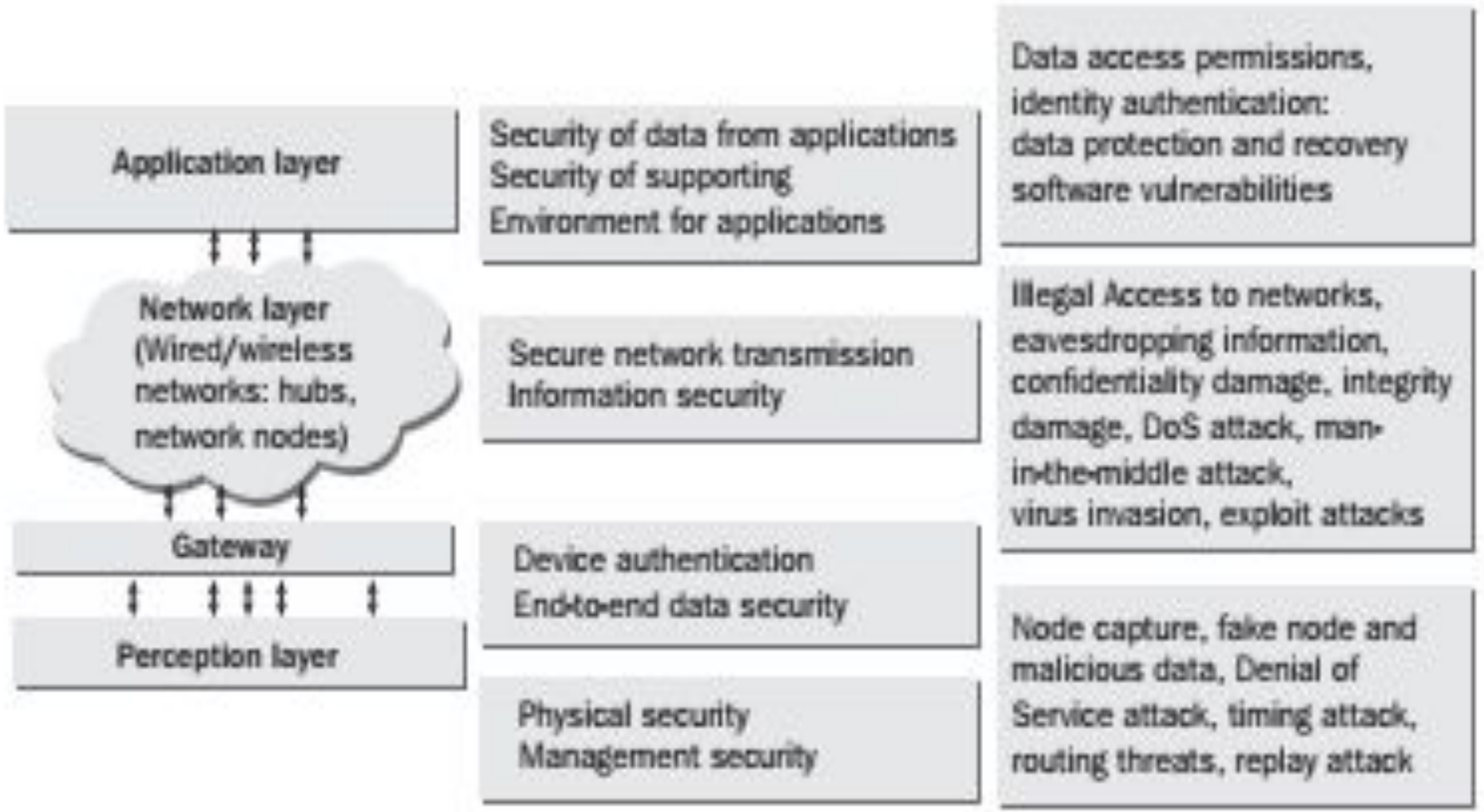


Process of Risk Assessment:

- Identifying Risks: We need to recognize possible issues, like unauthorized access or data breaches. It's like making a list of things that could cause problems.
- Evaluating Risks: Once we have the list, we look at each item and think about how bad it could be and how likely it is to happen.

Source : https://www.mdpi.com/1999-5903/13/6/148

Device Authentication and Authorization



1. Ensuring Trust:

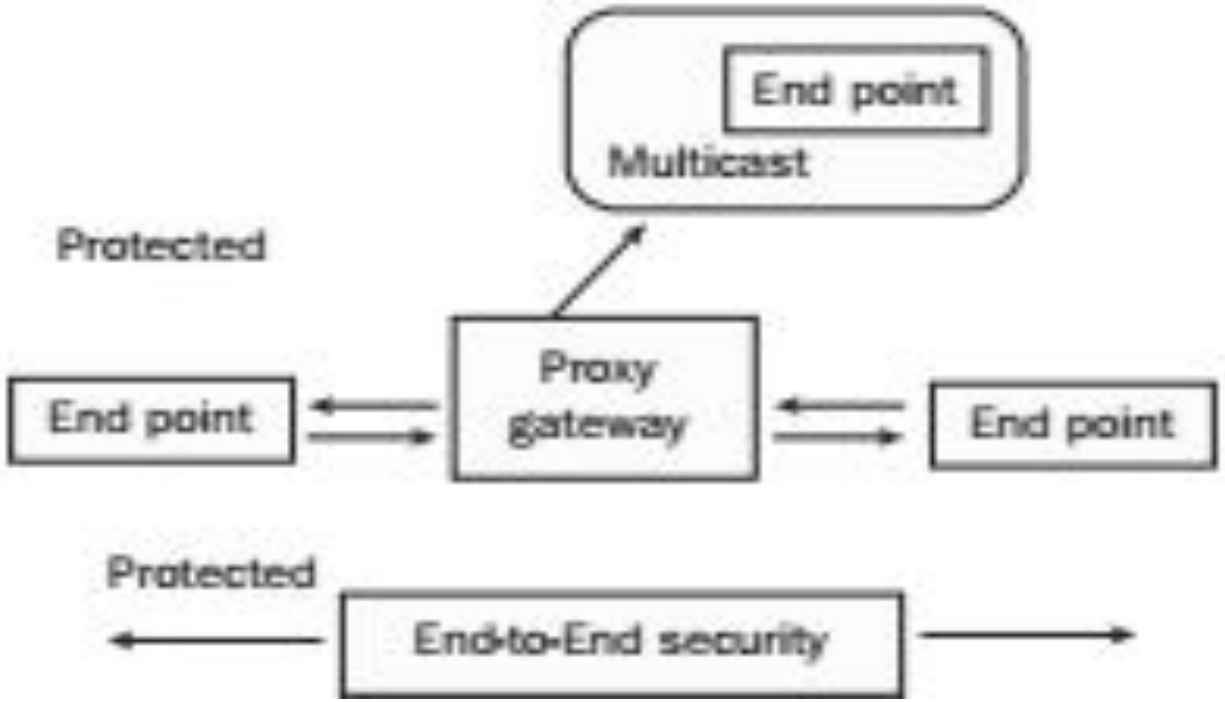
- Device authentication is like the digital ID card for IoT devices.
- It verifies the identity of each device in the network.

2. Authorization Protocols:

- Once a device is authenticated, it's essential to define what actions it is allowed to perform.
- Authorization ensures that even authenticated devices adhere to predefined rules, preventing misuse and maintaining the integrity of the IoT system.

Source : Joglekar, Jyoti; Durbha, Surya. Internet Of Things (p. 335). Kindle Edition.

Encryption for Data Protection



Source :Durbha, Surya. Internet Of Things (p. 341). Kindle Edition.

- Encryption is like a secret code. It scrambles our data so that even if someone tries to peek at it, they can't understand it without the right "key."
- End-to-end encryption Transportation Layer Security (TLS) is an industry standard layer for communication to send encrypted data over wide area network

ENCRYPTION FOR DATA PROTECTION

Role in Safeguarding Data:

- Imagine your smart thermostat sends data to the cloud about your home's temperature.
- With encryption, even if someone intercepts this data, they can't make sense of it without the special code.

End-to-End Encryption:

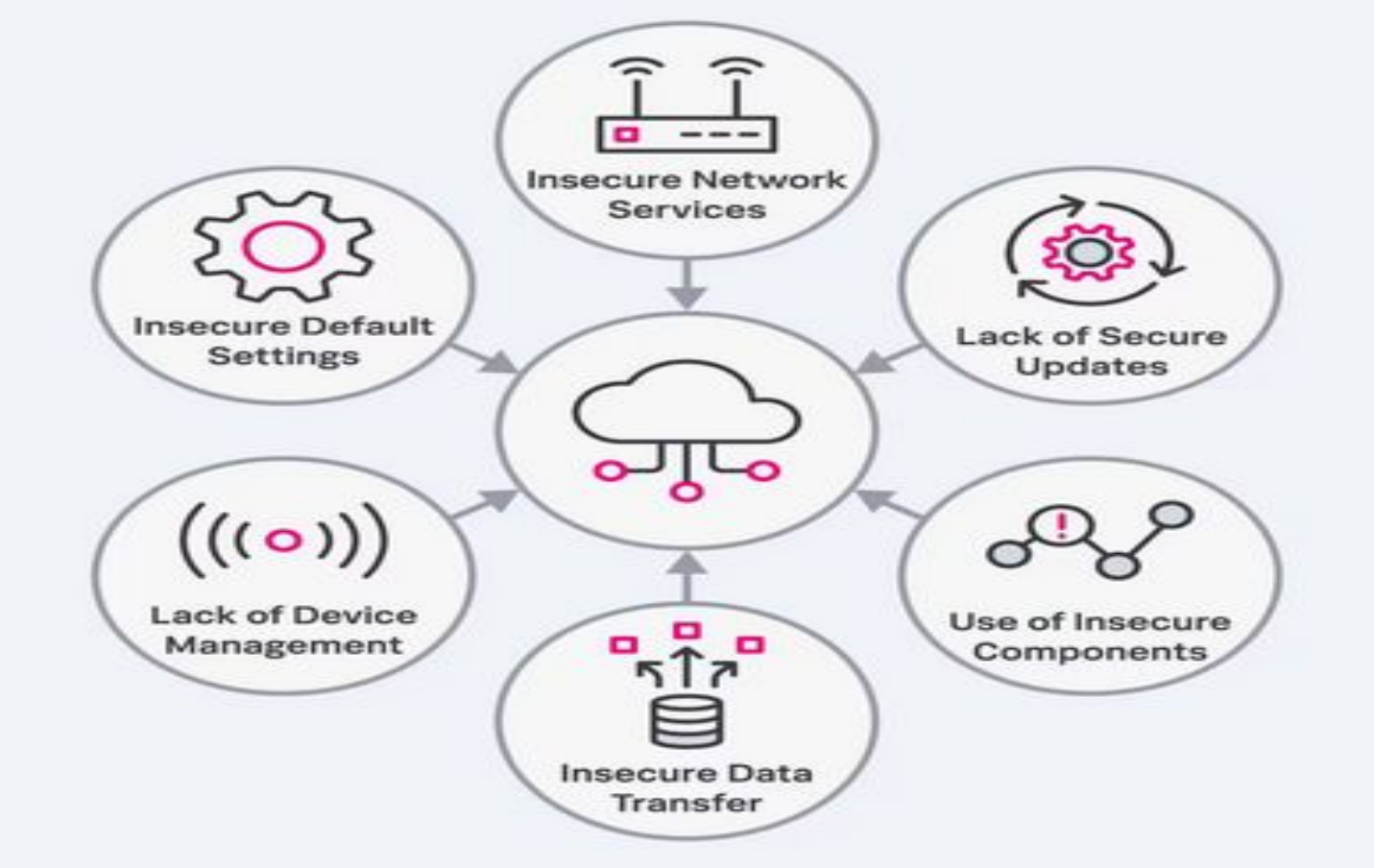
- We take it a step further with something called "end-to-end encryption."
- This means the data is protected all the way from your device to where it's supposed to go, ensuring its safety throughout the entire journey.

Continuous Security Monitoring

Adaptive Security:

- In the dynamic landscape of IoT, security is not a one-time task but an ongoing process.
- Continuous security monitoring involves adapting and adjusting security measures in response to the changing environment of IoT devices and networks.

Continuous Security Monitoring



Detecting Anomalies:

- Monitoring is like having a watchful eye over the IoT ecosystem.
- It helps in identifying anomalies or unusual activities that might indicate a security threat.
- By constantly observing patterns and behaviors, we can swiftly detect deviations that might signal potential security risks.

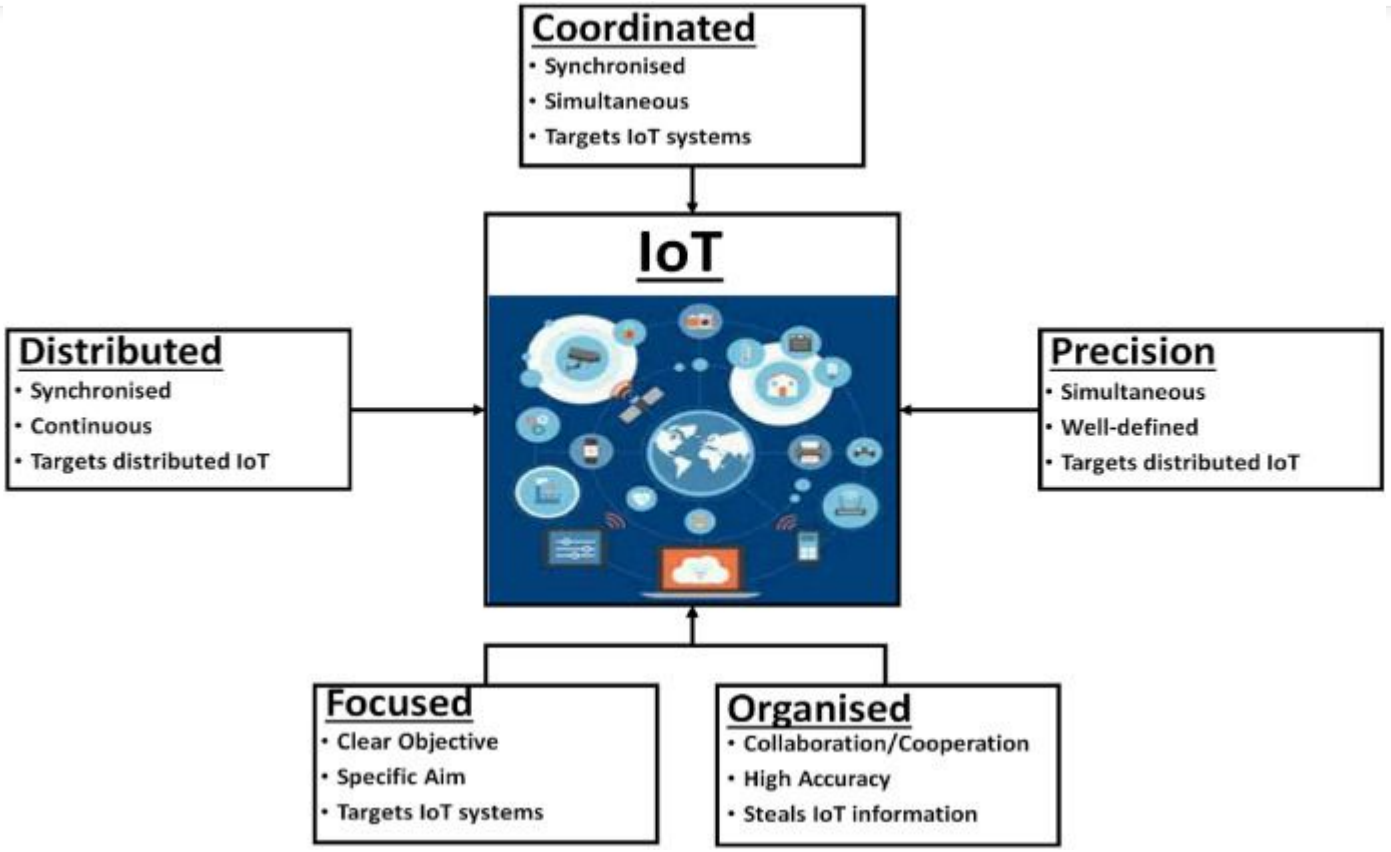
Source : https://www.splunk.com/en_us/blog/learn/iot-monitoring.html

Continuous Security Monitoring

Timely Responses:

- The real power of continuous security monitoring lies in its ability to facilitate timely responses.
- If an anomaly is detected, immediate action can be taken to investigate, address, and mitigate the potential security threat before it escalates.
- This proactive approach minimizes the impact of security incidents.

Continuous Security Monitoring



Dynamic Nature of IoT:

- IoT environments are characterized by a multitude of devices, each with its own set of interactions.
- Continuous monitoring acknowledges this complexity and ensures that security measures remain effective as the IoT ecosystem evolves over time.

Source :https://www.sciencedirect.com/science/article/pii/S2667345223000238

Continuous Security Monitoring

Risk Reduction:

- Ultimately, the goal of continuous security monitoring is to reduce risks associated with IoT devices and networks.
- By staying vigilant and adaptive, organizations can stay one step ahead of potential security issues, enhancing the overall resilience of their IoT infrastructure.

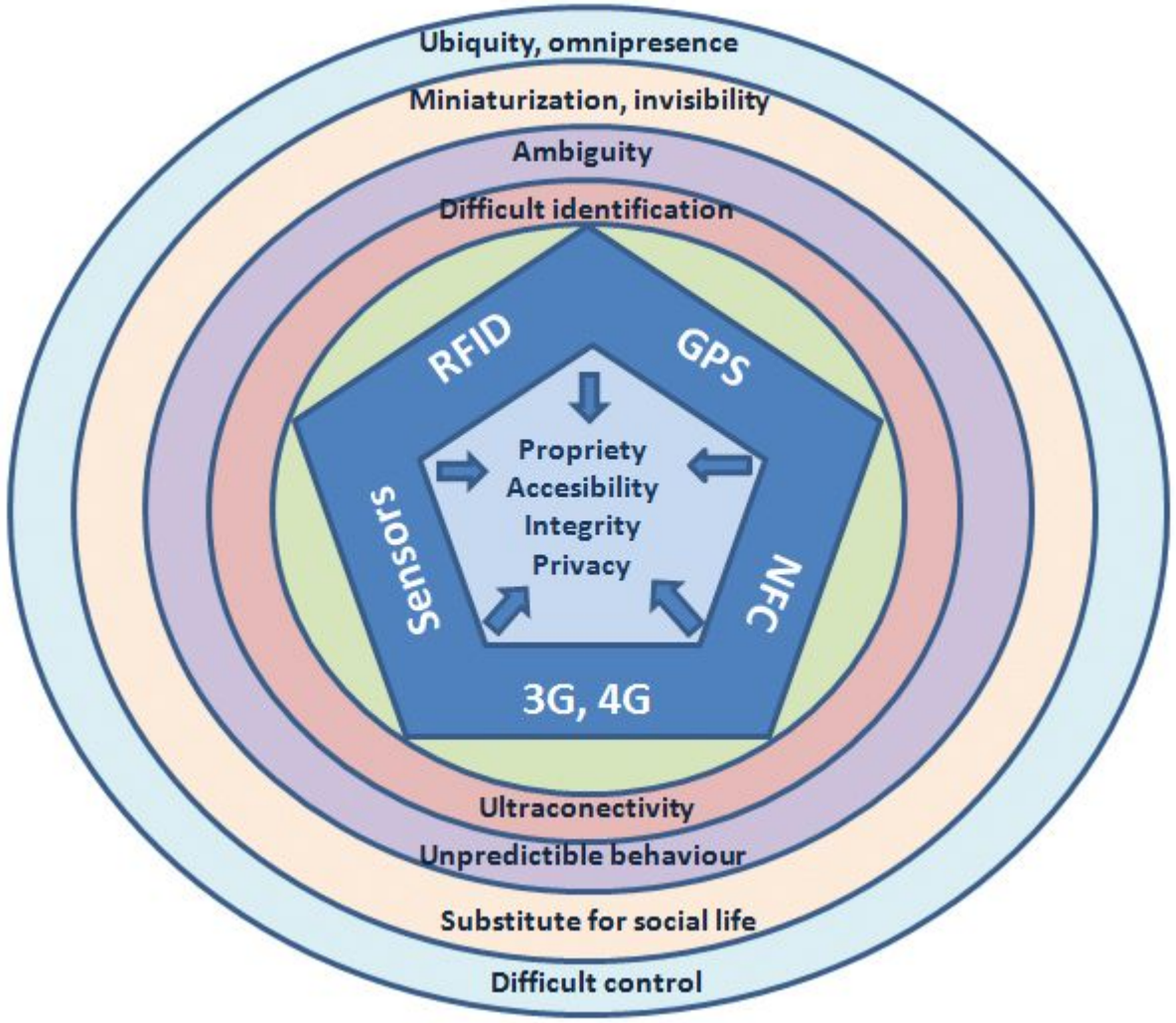
MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

Data Privacy and Ethical consideration in Data Management

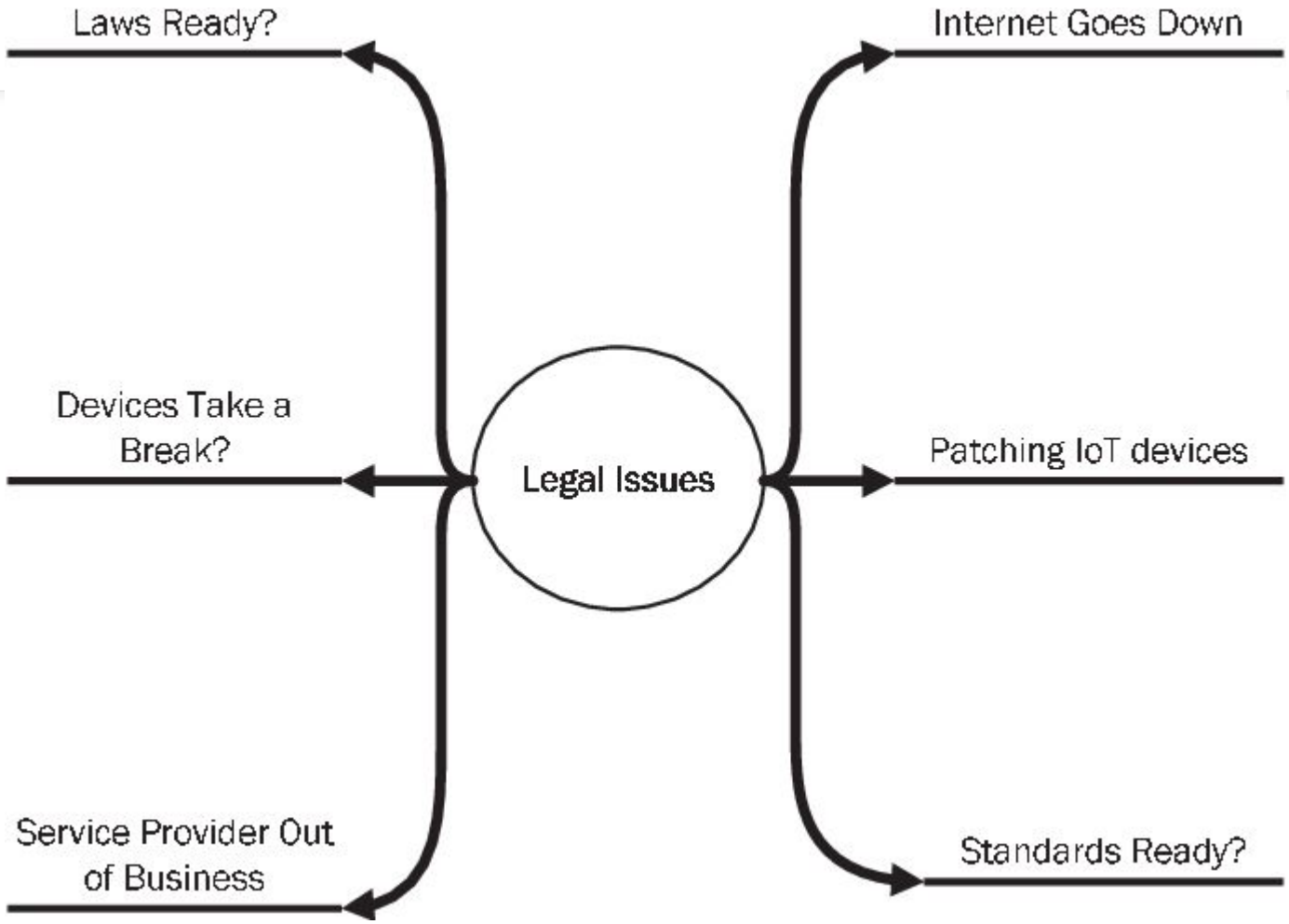
Introduction



https://www.researchgate.net/publication/260290933

- Data privacy and ethical considerations are critical aspects of data management in the Internet of Things (IoT) ecosystem.
- As IoT devices collect and process vast amounts of data, often involving personal information, it is essential to address these concerns to ensure responsible and secure use of data.

Informed Consent:



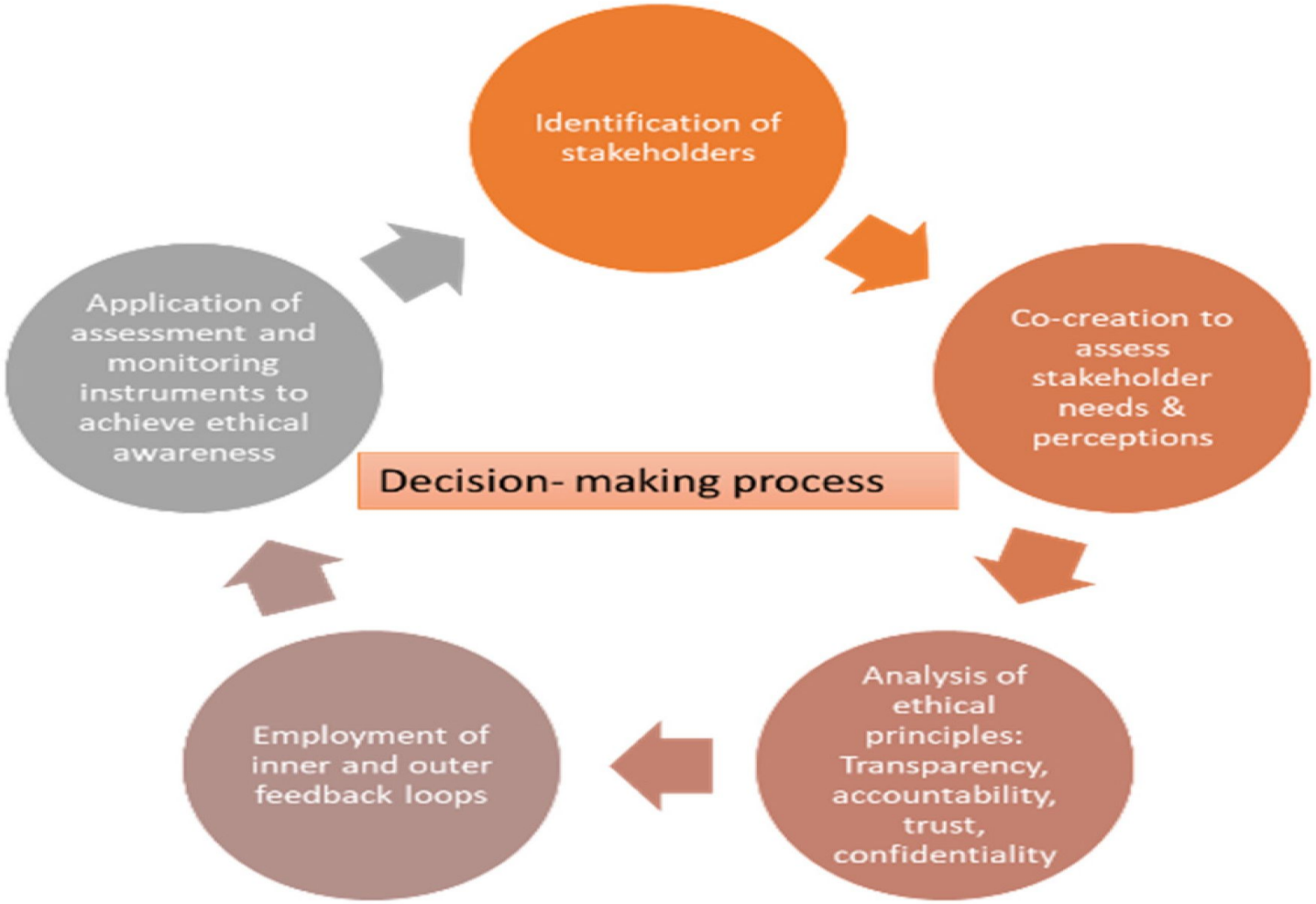
- Data Privacy: Obtain explicit and informed consent from individuals before collecting and processing their data. Users should be aware of what data is being collected, how it will be used, and have the option to opt in or opt out.
- Ethical Consideration: Respect the autonomy and privacy preferences of individuals. Provide clear and easily understandable information about data practices, allowing users to make informed decisions about their data.

Source: https://www.semanticscholar.org/paper/IoT-ethics-challenges-and-legal-issues

Transparency:

- Data Privacy: Be transparent about data practices, including the types of data collected, purposes for collection, and data-sharing arrangements. Provide users with clear information about how their data will be used.
- Ethical Consideration: Transparency is a cornerstone of ethical data management. Open communication fosters trust and allows individuals to make informed decisions about sharing their data.

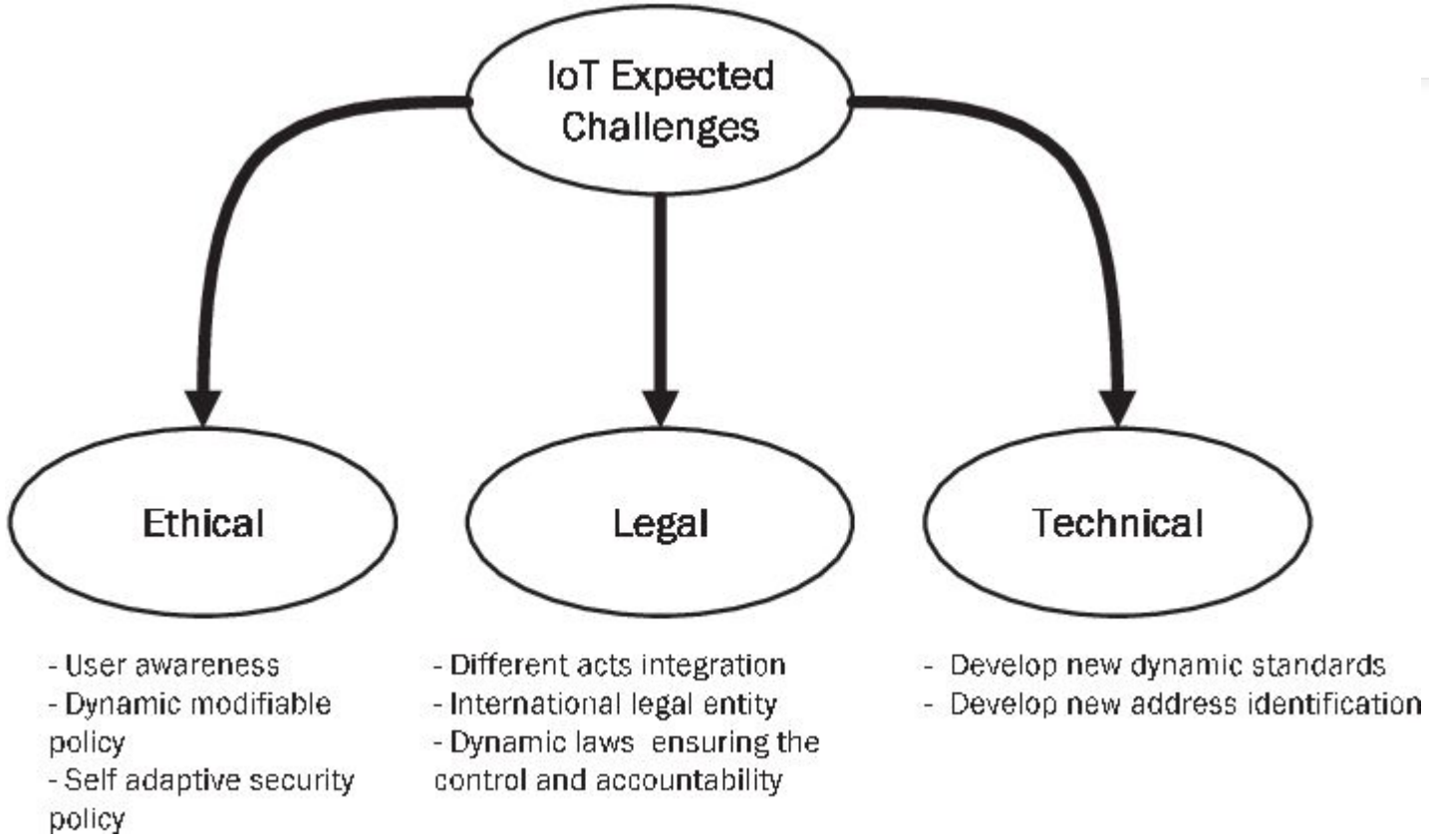
User Control and Access:



- Data Privacy: Empower users with control over their data. Allow them to access, correct, or delete their information. Provide mechanisms for users to manage their privacy settings.
- Ethical Consideration: Respecting user autonomy involves giving individuals control over their data. Ethical data management includes enabling users to exercise their rights regarding the collection and use of their personal information.

Source : https://fastercapital.com/topics/ethical-considerations-in-data-mining

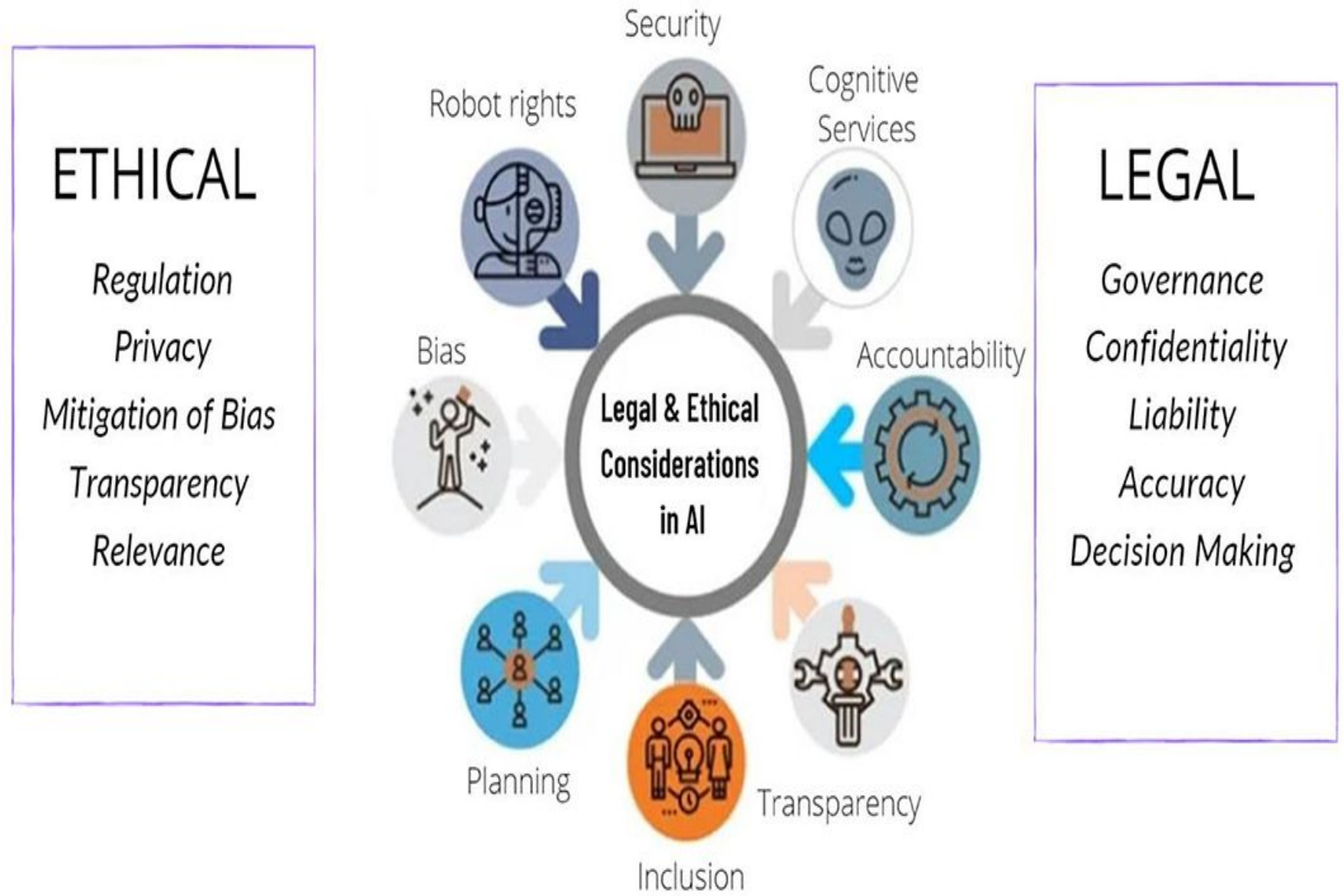
Regulatory Compliance:



Source : https://www.semanticscholar.org/paper/IoT-ethics-challenges-and-legal-issues

- Data Privacy: Adhere to relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or other regional privacy laws. Ensure that data management practices align with legal requirements.
- Ethical Consideration: Ethical data management goes beyond compliance with regulations. It involves a commitment to moral principles and practices that prioritize the well-being of individuals and communities.

Ethical AI and Algorithmic Decision-Making:



- Data Privacy: Ensure that algorithms and AI systems used in conjunction with IoT data are transparent, explainable, and accountable. Avoid discriminatory practices and biases in algorithmic decision-making.
- Ethical Consideration: Ethical AI practices involve considering the potential societal impact of algorithmic decisions. Evaluate and mitigate biases to promote fairness and prevent discrimination.

Source :https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322/full

MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

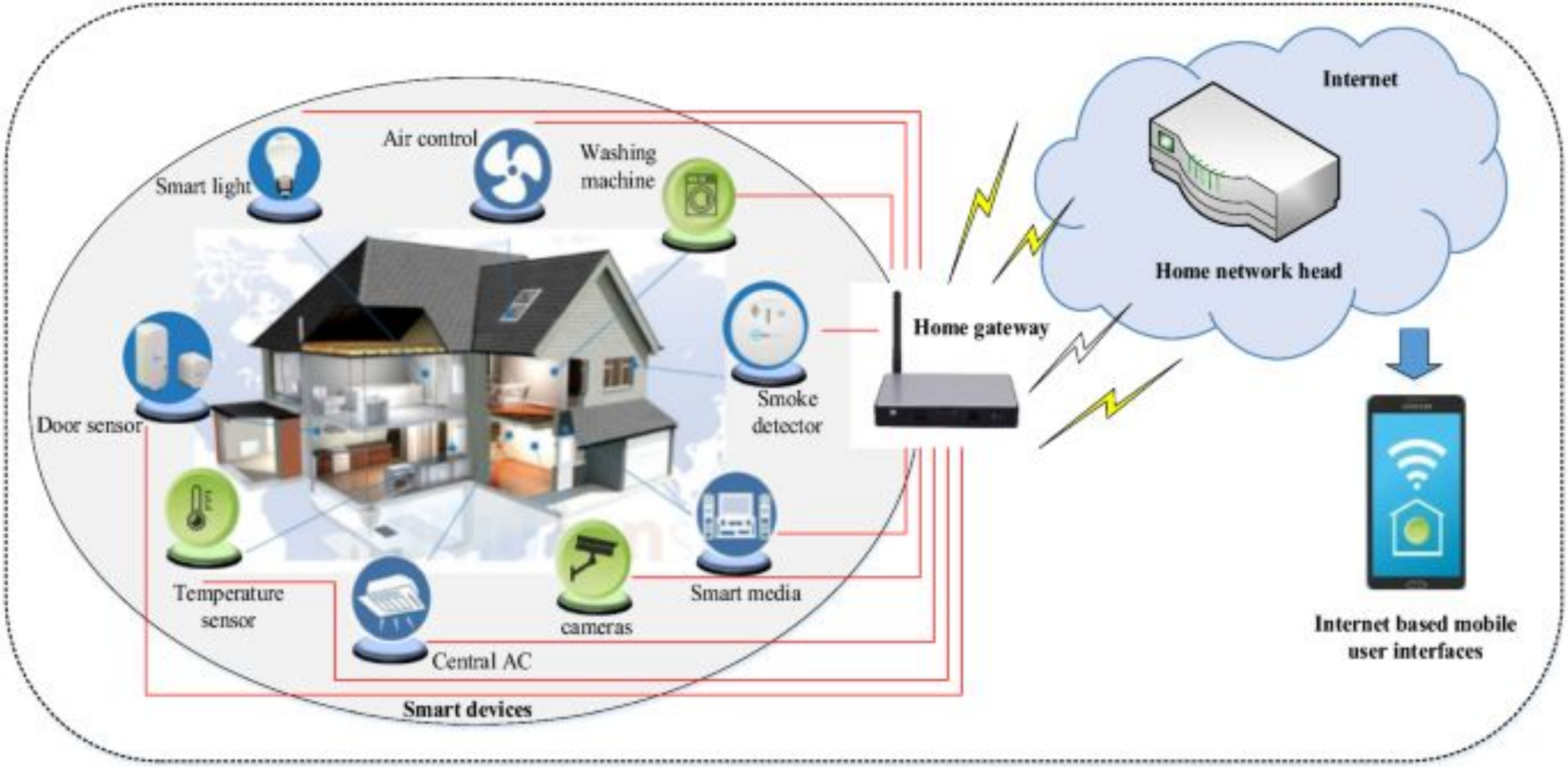
FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

Enhancing Security for Smart Home Devices

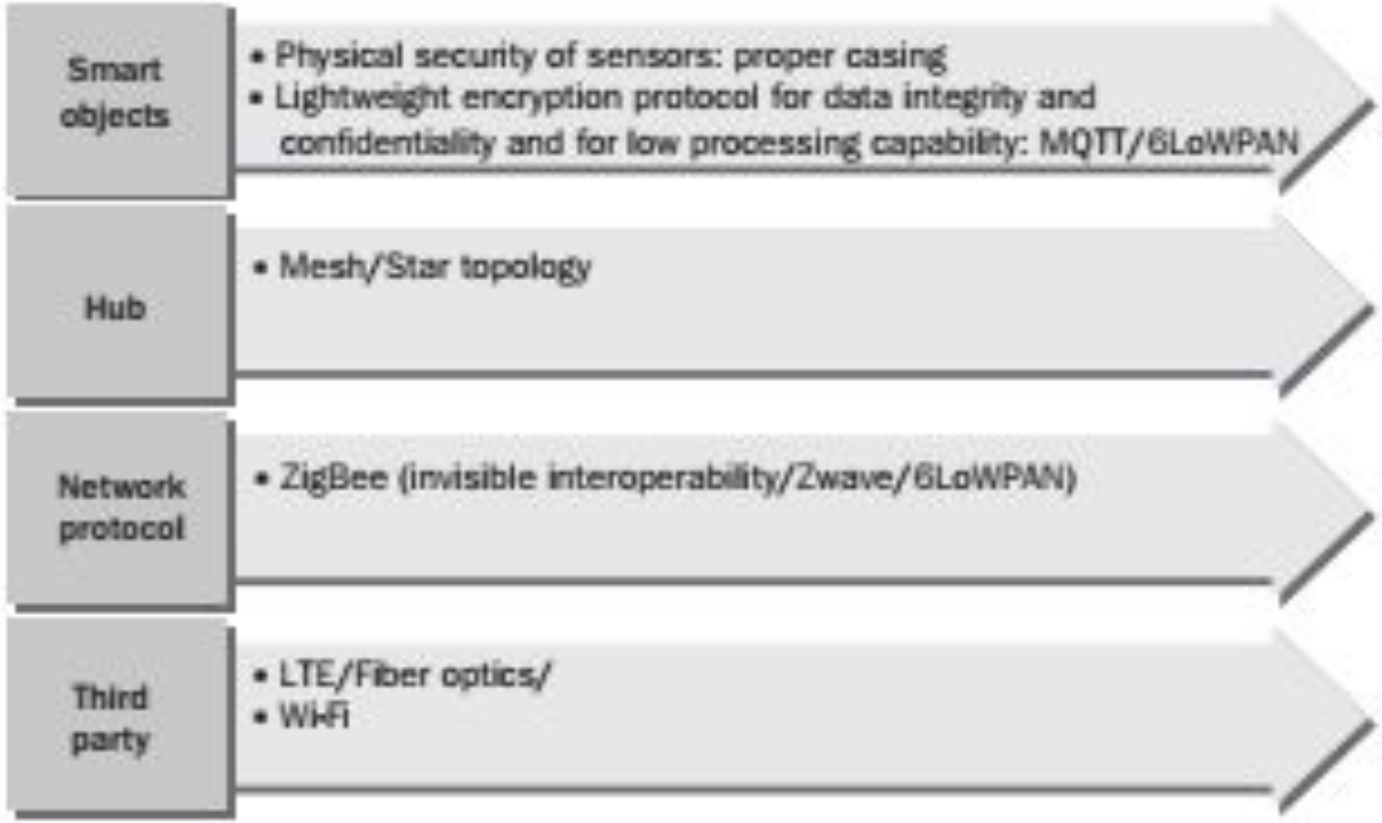
Case Study:

Smart Home Security System



Source : https://link.springer.com/article/10.1007/s11276-022-03197-1

overview



- ABC Security Solutions is a company that provides smart home security systems.
- Their IoT-based devices include smart cameras, door locks, and motion sensors, all connected to a central control hub.
- The company identified the need to strengthen the security of their devices after reports of unauthorized access and potential data breaches in similar systems.

Source : Durbha, Surya. Internet Of Things (p. 350)

Risk Assessment - Identifying Risks

- In the context of our hypothetical case study for ABC Security Solutions' smart home security system, the first step is the critical process of identifying potential risks associated with the IoT devices.
- This step involves a thorough examination of the system to pinpoint areas where vulnerabilities and threats could compromise security.

Risk Assessment

Examination of Potential Impact:

- Privacy Concerns: The compromise of user privacy emerged as a potential consequence, especially if unauthorized access to smart cameras occurred.
- Physical Security Breaches: The risk of physical security breaches was considered, especially if unauthorized users could manipulate door locks or gain control over the central hub.
- Severity of Impact: Assess the potential impact of each identified risk on the security and functionality of the smart home security system.
- Likelihood of Occurrence: Evaluate the likelihood of each risk actually occurring.

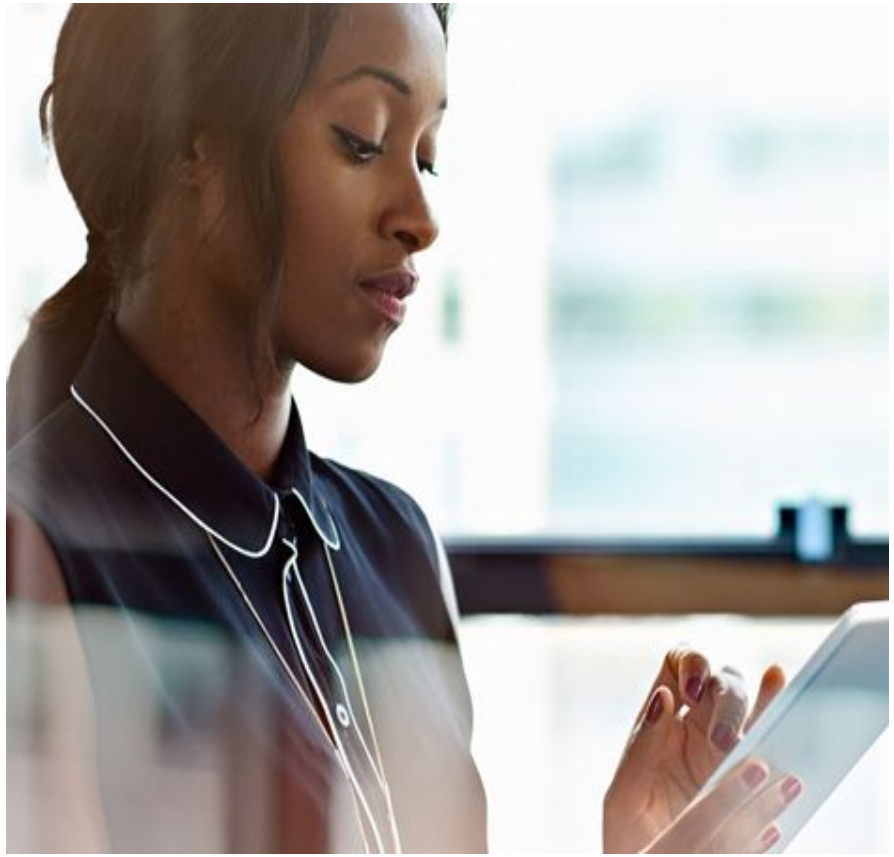
Continuous Improvement

Regular Security Audits:

- Scheduled Audits: Conduct regular security audits to identify and address new vulnerabilities. These audits can include penetration testing, code reviews, and system-wide assessments.
- Third-Party Assessments: Consider engaging third-party security experts to provide an objective evaluation of the system's security posture.

Summary

- IoT rapid progression many threats in security and privacy exists, which hinder its development.
- Explored the security goals required for a secure IoT system, and classified its security challenges and issues using a new unique classification method consisting of four classes of attacks; Physical, Network, Software, and Encryption Attacks.



MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

Python lab session

Connecting to a database & querying

MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

1. What are the challenges to provide security for IoT system.
2. Why data privacy is of prime importance in IoT systems?
3. Why lightweight cryptography is needed for IoT systems?
4. Explain two IoT security controls for middleware platform.