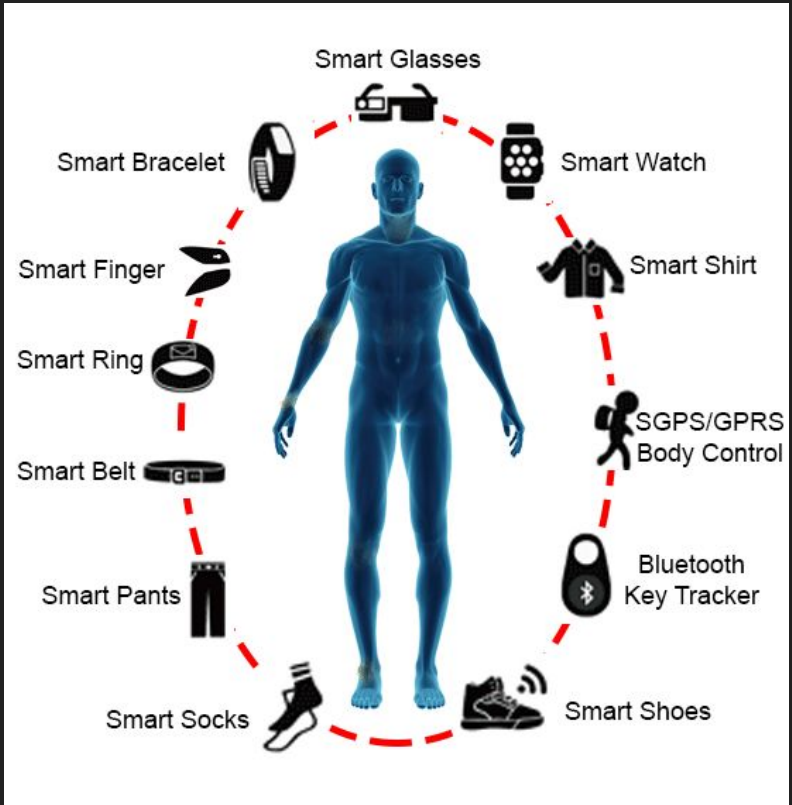
Remote Patient Monitoring System

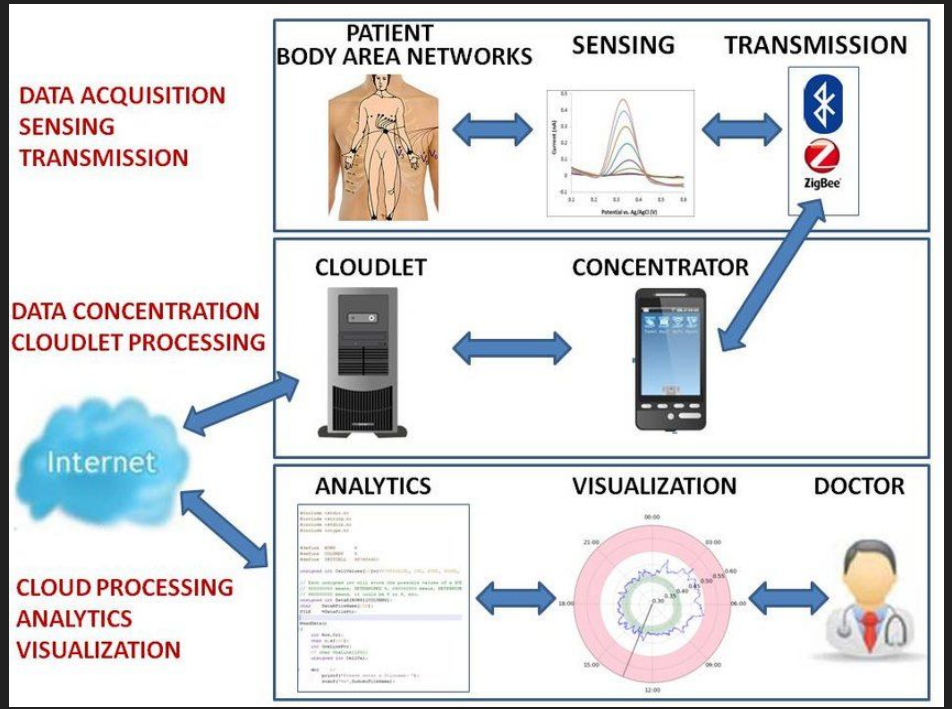
Elisa Veloso and Adam Roque

Remote Patient Monitoring System

- Remote monitoring technologies are adopted by homecare, clinicians, and hospitals environments to remotely monitor the vital signs of an individual communicating in real-time to patients, parents and physician a possible abnormality.
- Basically, these applications include a user interface (smartphones, tablets, and computers), a data collector (biosensors), and Internet connectivity. In this regard, it can be performed with the integration of IoT, mobile computing and cloud storage and it aims to turn available the visualization of the data in real-time.

Remote Patient Monitoring System





2 : Security Threats

1. Man-in-the-Middle Attack :

- **Description**: During transmission from the device to the smartphone or from smartphone to cloud, an attacker intercepts and possibly alters the data.
- **Impact**: Compromised medical data, false readings, or missed alerts, risking patient health.

2.Unauthorized Access to Patient Records

- **Description**: Attackers gain access to backend systems via weak authentication or misconfigured access controls
- **Impact**: Leakage of sensitive medical data, Violation of privacy and regulatory compliance, Identity theft using personal health information ,loss of trust in the healthcare provider.

3. Device Tampering / Firmware Exploits

- **Description**: Physical or remote tampering of IoT device firmware to manipulate data or gain backdoor access.
- **Impact**: Malfunctioning device, false diagnostics, potential control of other connected systems.

3 : Security Measures

1. End-to-End Encryption:

- **Use**: Encrypt data during transmission and at rest.
- **Effectiveness**: Prevents Man in the middle attacks

2.Strong Authentication & Access Control

- **Use**: Multi-factor authentication, role-based access for his users.
- **Effectiveness**: Ensures only authorized personnel can access or modify records.

3. Secure Firmware & Regular Updates

- **Use**: Digitally signed firmware, OTA updates, tamper-detection.
- **Effectiveness**: Reduces risks from firmware vulnerabilities and device-level attacks.

References:

- https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
- https://www.hhs.gov/hipaa/for-professionals/security/index.html
- RODRIGUES, Joel J. P. C. et al. Enabling Technologies for the Internet of Health Things. IEEE Access, v. 6, p. 11375–11388, 2018. DOI: 10.1109/ACCESS.2017.2789329. Disponível em: https://www.researchgate.net/publication/322261039_Enabling_Technologies_for_the_Internet_of_Health_Things. Acesso em: 20 maio 2025.
- ResearchGate
- RODRIGUES, Joel J. P. C. et al. Different types of wearable technology [graphic]. In: RODRIGUES, Joel J. P. C. et al. Enabling Technologies for the Internet of Health Things. IEEE Access, v. 6, p. 11375–11388, 2018. Figure 5. DOI: 10.1109/ACCESS.2017.2789329. Available at: https://www.researchgate.net/figure/Different-types-of-wearable-technology_fig5_322261039. Accessed on: 20 May 2025.
- SOYATA, Tolga. Components of a remote patient monitoring system that is based on an IoT-Cloud architecture [graphic]. In: SOYATA, Tolga. Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. [S.l.]: [s.n.], 2015. Figure 1. Available at: https://www.researchgate.net/figure/Components-of-a-remote-patient-monitoring-system-that-is-based-on-an-IoT-Cloud_fig1_280924370. Accessed on: 20 May 2025.
- IoT Security today’s lecture

Thank You