In the Internet-of-Things (IoT) physical devices are embedded with electronic components achieving sensory, computational, storage and communication capabilities.

In IoT-based applications, devices are spread along large scale networks in which they collect and exchange a big amount of data. These data are used to make rapid decisions and analysis.

In such a scenario, properties like availability, portability and fast communication are necessary. To achieve them, the acting devices must integrate light communication and encryption protocols, preferring availability and performances over computational power and security.

Achieving security in IoT-based applications is challenging due to a lack of resources and vulnerable protocols. Such applications interconnect a number of technologies, i.e. Communication and Information systems (CIS), like cloud computing, network communication protocols, cryptography and physical systems. Each of these components comes out with a number of vulnerabilities which may affect the system.

The fulfilment of IoT systems should come out with mitigation strategies and strong analysis of the risks and benefits. However, because the complex nature of such systems, most of the time these tasks are difficult to accomplish, causing a waste of money and resources for the industries.

Security Approach:

According to the OWASP IoT Project\(^1\), we propose:

1. Classify the most common IoT attack surface areas (Figure 1),
2. Identify the most dangerous vulnerabilities (red line in Figure 1),
3. Propose a security methodology (Figure 2)

---

Figure 1. Classification of the attack surface areas

\(^1\) https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Figure 2. Security methodology

\(^2\) https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas