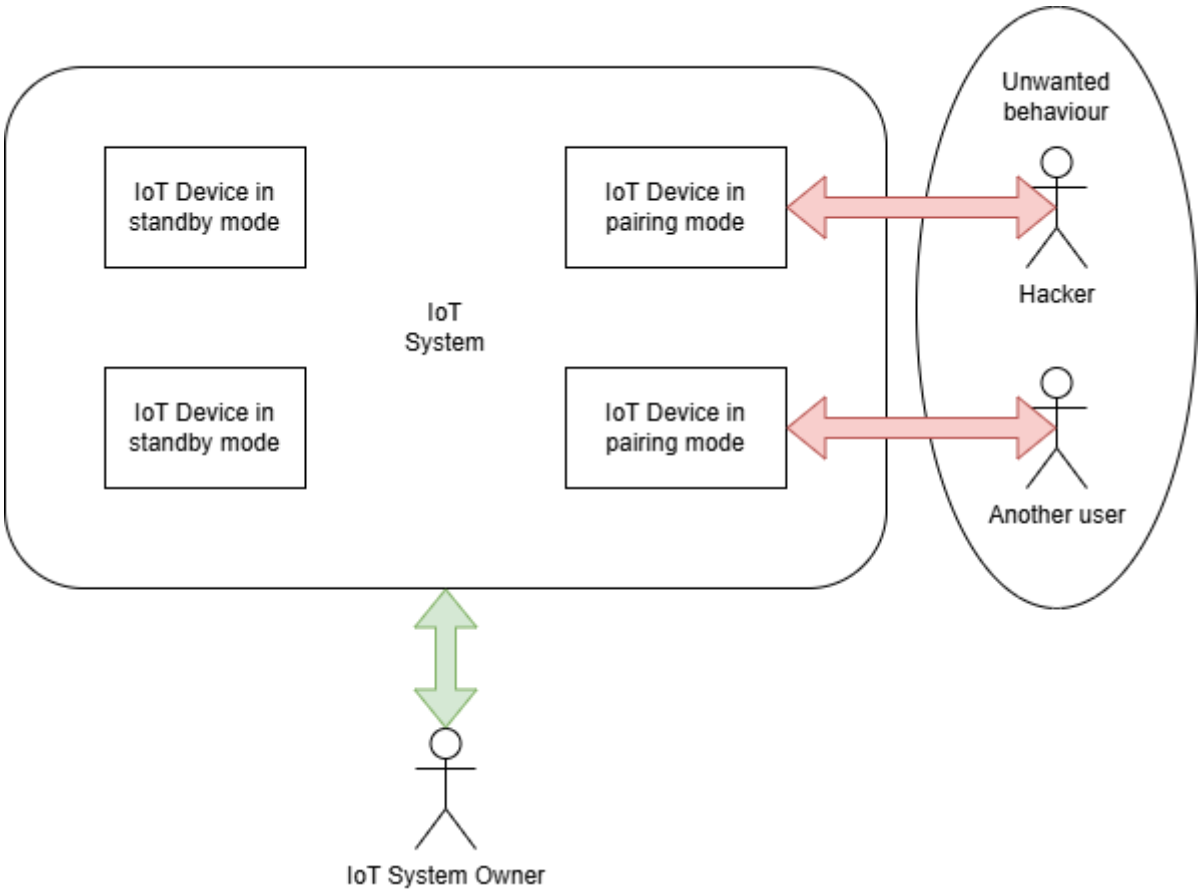
Precise Problem Description

The rapid growth of smart-home technologies has led to an increasing number of interconnected IoT devices inside private households. According to recent industry analyses, more than 21 billion IoT devices will be in use globally by the end of 2025. While these devices bring convenience and automation, they also introduce significant vulnerabilities. Many consumer IoT devices have weak or inconsistent security standards, rely on outdated authentication methods, or use shared default keys. As a result, smart homes are becoming increasingly exposed to unauthorized access, data interception and manipulation by external actors.

Current smart-home ecosystems lack a **consistent, secure and user-controlled method** for onboarding and authenticating devices. Users have little transparency or control over how their devices are connected and the way data is transmitted and protected. This creates a fragile security environment in which attackers can exploit devices in pairing mode to access private information, monitor household behaviour patterns or even gain control over them.



This problem threatens the fundamental expectation that a home is a **safe, private, and protected space**. Without a reliable, standardized security mechanism, users cannot be certain that their personal data remains confidential or that their smart-home devices are safeguarded against unauthorized external access.