# IoT Security and Privacy Case Study Report

## Introduction

The Internet of Things (IoT) has transformed homes, agriculture, healthcare, and industry by enabling real-time data collection and automation. However, the increasing number of connected devices has also introduced significant security and privacy risks. Many IoT systems are deployed with weak protection mechanisms, making them vulnerable to cyber-attacks and misuse of personal data. This report identifies three major IoT vulnerabilities, proposes two security controls, and discusses one ethical/privacy concern related to IoT usage.

## Major IoT Vulnerabilities

### 1. Weak Authentication and Default Passwords

Many IoT devices are shipped with default usernames and passwords that users rarely change. Attackers can easily exploit this to gain unauthorized access to devices such as smart cameras, routers, and home automation systems. Once compromised, these devices can be used for spying, data theft, or participation in botnet attacks.

### 2. Unencrypted Communication

Some IoT devices transmit data without encryption, especially when using simple protocols like HTTP instead of HTTPS or MQTT without TLS. This makes it possible for attackers to intercept sensitive information such as location data, health readings, or home activity patterns.

### 3. Lack of Firmware Updates

Many IoT manufacturers do not provide regular security updates for their devices. As a result, known vulnerabilities remain unpatched, allowing hackers to exploit weaknesses long after they are discovered.

## Proposed Security Controls

### 1. Strong Authentication and Access Control

Users should be required to change default passwords and use strong authentication methods such as multi-factor authentication (MFA). Device access should be limited to authorized users only.

### 2. Encrypted Communication (TLS/HTTPS)

All data transmitted between IoT devices, cloud platforms, and dashboards should be encrypted using secure protocols like HTTPS or MQTT with TLS. This prevents eavesdropping and data tampering.

## Ethical and Privacy Issue: Smart Home Surveillance

Smart home devices such as cameras, voice assistants, and motion sensors can collect continuous data about users’ daily activities. While this improves security, it also raises privacy concerns because companies or hackers could misuse this data. Users may be monitored without their full awareness, leading to potential violations of personal privacy. Therefore, IoT designers should ensure transparency, user consent, and strong data protection policies.

## Conclusion

While IoT offers significant benefits, its security risks must be addressed through better device design, encryption, and user awareness. Protecting IoT systems is essential to prevent cyber threats and safeguard personal privacy.