EE450 Survey Proposal

Security and Privacy Issues in the Internet of Things

İsmail Akbaş
S024094

Hasan Alp Doyduk
S025015

Security and Privacy Issues in the Internet of Things: A Survey

İsmail Akbaş – S024094
Hasan Alp Doyduk – S025015

1. Project Description and Goals

This survey project aims to investigate security and privacy issues in IoT (Internet of Things) environments, focusing on common threats, countermeasures, and current research directions. As IoT technologies rapidly expand across domains such as healthcare, smart homes, transportation, and industrial automation, securing data and ensuring user privacy have become critical challenges. The decentralized and heterogeneous nature of IoT systems increases their vulnerability to various attacks, including device hijacking, data tampering, firmware manipulation, and unauthorized access.

The goals of this survey:

- Provide a detailed overview of the layered security architecture of IoT, including the perception, network, and application layers.
- Identify significant security and privacy vulnerabilities specific to IoT systems.
- Examine contemporary methods such as federated learning and post-quantum cryptography for enhancing IoT security.
- Review existing access control models and suggest future directions for fine-grained, decentralized policy enforcement.

Our final deliverable will consist of a structured, literature-supported survey that not only summarizes current solutions but also highlights unresolved research questions in securing IoT ecosystems.

2. Motivation

The motivation behind this project arises from the increasing integration of IoT technologies into critical aspects of daily life and industry, such as smart homes, healthcare systems, agriculture, and industrial control systems. While IoT enables real-time data collection and intelligent automation, it also presents significant privacy and security risks due to its distributed nature, low-resource devices, and complex communication protocols.

Unlike traditional computing systems, IoT devices often lack robust security mechanisms, making them prime targets for cyberattacks, such as unauthorized access, data breaches, and remote code execution. Attacks on IoT systems can lead not only to leaks of sensitive data but also to physical consequences, for example, hijacking a smart medical device or disrupting a city's smart grid.

Moreover, regulatory frameworks like GDPR and CCPA are increasingly demanding secure management of user data, urging researchers and developers to create systems that are both privacy-preserving and transparent.

The urgency of this research stems from several critical factors. First, the rapid proliferation of billions of interconnected IoT devices has significantly expanded the potential attack surface, making these systems

increasingly vulnerable. Second, many IoT devices operate under strict resource limitations, creating a pressing need for lightweight and scalable security solutions that can function effectively within these constraints. Lastly, as IoT technologies become more integrated into everyday life, it is essential to establish transparent and auditable security frameworks that help maintain user trust and ensure responsible data handling.

3. Milestone and Timeline

To complete this survey, we will first collect academic sources related to IoT security and privacy, focusing on recent papers published in reputable journals. After gathering the literature, we will organize the information based on common themes such as security issues in different IoT layers and modern defense techniques like blockchain, federated learning, and firmware analysis. We will then summarize and compare the methods presented in the literature, highlighting their strengths, limitations, and areas where further research is needed. Finally, we will review and revise the document to ensure it is clear, well-structured, and aligned with the project goals.

4. References

Sun P., Wan Y., Wu Z., Fang Z., & Li Q. (2025). *A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions*. Computers & Security, 148, 104097. https://doi.org/10.1016/j.cose.2024.104097

Arakadakis K., Charalampidis P., Makrogiannakis A., & Fragkiadakis A. (2021*). Firmware Over-the-air-Programming Techniques for IoT Networks - A Survey.* ACM Computing Surveys, 54(9), 1–36. https://doi.org/10.1145/3472292

Manifavas C., Hatzivasilis G., Fysarakis K. & Rantos K. (2013). *Lightweight Cryptography for Embedded Systems – A Comparative Analysis.* https://www.researchgate.net/publication/256476517_Lightweight_Cryptography_for_Embedded_Systems_-_A_Comparative_Analysis