DOI https://doi.org/10.30525/978-9934-26-459-7-8

PRIVACY AND SECURITY IN THE INTERNET OF THINGS ERA

Mert Bahce
ISMA University of Applied Sciences, Latvia
**Corresponding author's e-mail: xmertbahce52@gmail.com*

Abstract

Since the third era of globalisation started by 1989 and continues today, according to United Nations Population Fund records approximately 8.5 billion people will be living in big cities by 2030. People are swarm into big cities for a new job, opportunities and better life standart. This situation causes big problems in cities such as urban sprawl, air pollution, waste of water sources, increasing criminal rates, traffic congestion, sustainability and so on and so forth. On the other hand, security and privacy concerns become a real problem, The increase of interconnected devices poses significant risks including cyberattacks, data breaches, unauthorised surveillance. We will address these crucial issues by proposing robust cybersecurity measures, data encryption protocols, privacy-enhancing technologies to decrease risks and build trust in IoT-enable smart city initiatives.

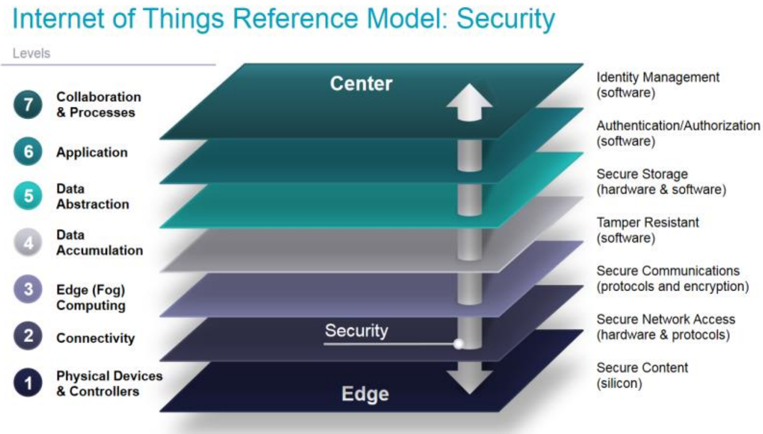
Key words: *Internet of Things, privacy, cyberattacks, protection protocols, vulnerability.*

1. Introduction

In today's digital world, the growing number of connected devices has brought about a big change in how technology advances and makes things easier.

IoT devices became a necessity for daily life, business models and even city planning. However besides all the benefits of IoT devices, there are some critical issues about privacy and security. The intertwining of privacy and security issues within the IoT ecosystem raises critical questions regarding the safety of personal information, the prevention of unauthorised access, the softening of potential risks and vulnerabilities.

We can see the reference model of IoT below.


Internet of Things Reference Model: Security
Levels
7 Collaboration & Processes
6 Application
5 Data Abstraction
4 Data Accumulation
3 Edge (Fog) Computing
2 Connectivity
1 Physical Devices & Controllers
Center
Security
Edge
Identity Management (software)
Authentication/Authorization (software)
Secure Storage (hardware & software)
Tamper Resistant (software)
Secure Communications (protocols and encryption)
Secure Network Access (hardware & protocols)
Secure Content (silicon)

Security is one of the most important requirements for an IoT system architecture. Somehow, it also happens to be one of the key challenges facing IoT architecture, and IoT devices themselves. Broadly, the IoT **security** layer comprises three main aspects:

- **Equipment Security:** involves the actual IoT devices, and protecting these endpoints from malware and hijacks
- **Cloud Security:** with most IoT data being processed in the cloud, cloud security is crucial to prevent data leaks
- **Connection Security:** focused on securing data transmitted across networks, primarily with encryption. The transport layer security (TLS) protocol is considered the benchmark for IoT connection security

We will dive into those aspects and provide the most efficient model for secure IoT devices.

Overview

The Internet of Things (IoT) has revolutionised the way we interact with technology, connecting billions of devices and generating huge amounts of data. However, this unprecedented connectivity also brings significant challenges in terms of privacy and security. In this thesis, we explore the evolving landscape of privacy and security in the IoT era, addressing key concerns, identifying common threats, and proposing mitigation strategies. By examining the intersection of technology, policy, and user behaviour, I aim to contribute to the development of robust solutions that safeguard individual privacy and enhance the security of IoT ecosystems.

Decision

The Internet of Things (IoT) connects lots of devices, like smart thermostats and fitness trackers, to make our lives easier. But sometimes, these devices can cause privacy and security problems. This thesis explores these issues and suggests ways to keep our information safe. We'll look at what goes wrong, what we can do about it, and how everyone—from regular people to big companies—can make smart choices to protect our privacy and security online.

Conclusion

In conclusion, this thesis has explored critical points of privacy and security in IoT. Through a comprehensive examination of emerging threats, vulnerabilities and mitigation strategies, gained valuable insights into the complexities of safeguarding IoT devices and ecosystems.

By advocating for robust security practices, such as encryption, authentication, and regular updates, we can enhance resilience against malicious actors and mitigate the risks posed by evolving cyber threats.

References

1. https://www.un.org/en/global-issues/population
2. https://dgtlinfra.com/internet-of-things-iot-architecture/
3. https://dl.icdst.org/pdfs/files4/0f1d1327c5195d1922175dd77878b9fb.pdf
4. https://dgtlinfra.com/internet-of-things-iot-architecture