IoT for Smart Home Environment: Security Challenges and Security Approaches

Duy Thuc Pham (101767225)

Faculty of Science, Engineering, and Technology, Swinburne University

Hawthorn, Australia

101767225@student.swin.edu.au

# INTRODUCTION

# REVIEW METHOD

# REVIEW OF RELATED WORKS

## Domain Overview

## Security Challenges

The authors claim that due to the significance of the private information containing in smart home systems, security requirements for them is essential. In order to find out the main challenges and threats in smart home systems, authors conduct a test to some of the smart home systems including Nest Learning Thermostat, Nest Smoke Detector, Samsung Smart TV, etc. Consequently, based on the analysis, they found out five main challenges in smart home systems: resource constraints, Heterogeneous Communication Protocols, Unreliable communications, Energy Constraints, Physical Access. They claim that the limitation of resource and energy are the main challenges for smart home systems. A strong merit of this article is to conduct an investigation of existing security threats in each OSI communication layer. Thereby, the authors asserted the need for further study to mitigate the attack from the malicious firmware.

Lin and Neil W.Bergmann2016 report that even though smart home systems are able to bring more comfort, security and ecological sustainability, there are plenty of challenges in smart home systems (SHS). They show that these challenges come from many factors such as networked system accessibility, system physical accessibility, system resources, system heterogeneity, fixed firmware and slow uptake of standards. Noticeably, they consider the most challenges to be a human factor, since there are no security professionals to operate the smart home network, and thus householders cannot afford to control their home network. In addition, a practical vulnerability example regarding how home surveillance cameras may be attacked by using Shodan – an IoT search engine – is provided to alert householders not to trust on smart home systems. However, the lack of quality data for each vulnerable factor in this research article makes these arguments less persuadable.

## Security Approaches

# CONCLUSIONS