Summary **IoT Privacy and Security Challenges for Smart Home Environments**

**Challenges**

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) (Lin and Neil W.Bergmann2016). 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.

Summary **Securing Smart Home: Technologies, Security Challenges, and Security Requirements**

**Challenges**

Changmin Lee∗, Luca Zappaterra∗, Kwanghee Choi∗†, and Hyeong-Ah Choi∗

The authors stress the crucial of security requirements in smart home systems due to the significance of the private information containing in a smart home systems. They provide a list in detailed specification of smart home devices as well as current communication protocols that has been used recently. Based on that, they rigorously investigate, and eventually conclude that there are five main security challenges in smart home devices such as resource constraints, heterogeneous communication protocols, unreliable communications, energy constraints and physical access. A good merit of this paper is to present clearly the security challenges in particular smart home devices, which is absolutely helpful for further study.

A good merit of this article is

. A good merit of this article is the author rigorously investigate each security challenges. They find out a list of smart home devices in detailed specification

Summary A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes

In order to improve the security and privacy for smart home systems, authors provide a security design for smart home systems. Also, they recommend that while transmitting data, a chaos-based cryptographic scheme and message authentication codes (MACs) should be combined to guarantee cybersecurity main themes such as confidentiality, data integrity and authentication. The main contribution of the paper is to provide a smart home design including four groups: appliance group, monitor group, central controller and user interfaces.

Summary Security **Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System**

**Summary A review of Internet of Things for smart home: Challenges and solutions**