# How Secure are Smart Homes

Jake Cunningham 001211278

## Introduction

Smart homes provide effortless control to devices such as include lightbulbs, thermostats, electrical outlets, or door locks. The main advantage of this is being able to control many aspects of the home from different connected devices either a click on a phone or over voice command from a smart speaker. Smart homes due to their internet connectivity can be controlled and monitored remotely from anywhere in the world, meaning complete control over a home at any time. However, with these advantages are also what can lead to significant risks. Hackers can exploit the technology that underlies these devices, and potentially compromise the user's privacy, granting unauthorized access, or even gaining complete control over the entire home system. This poses a severe threat to privacy and safety within a person's home.

It has been reported over the years cases of smart devices being hacked, with exploits as simple as not changing the default login details. (Hill, 2013) Some smart devices don't even attempt to install privacy, using a website such as exploit-db., any user is able to find publicly available Ip address that have been crawled and logged on google. Often this means that complete strangers can find and monitor and sometimes even manipulate Ip cameras without any security protections.

There may be good news however, in 2024 a new law in the United Kingdom was passed that meant any smart devices sold in the UK would have to follow stricter laws that ensure that protection of users. This includes removing default passwords making sure that users have entered a unique password and making clear how long devices are supported with security patches and under warranty (Hooker, 2024)

# Use case scenario and background.

Smart homes were developed to make peoples lives easier and more efficient, the use of By integrating the Internet of Things (IoT) and IOT connected devices means that people can have access to their homes anytime and anywhere with either their smartphone or simply their voice on a smart speaker.

A modern smart home may contain devices such as, Smart Locks, Doorbells, CCTV that can all improve the safety and security of a property as well as providing cost effective ways of monitoring house without any invasive infrastructure. Smart thermostats so that heating is able to be controlled anywhere meaning a home can be preheated before arriving, automated lighting can cut energy  costs by learning the routines of households of  and Smart fridges that are able to provide recipes and available ingredients right on the front.

Machine learning is a key aspect of many of the features of the smart home devices, it enables these devices to process vast amounts of data, learn user preferences, and predict behaviours, which enhances their functionality. For instance, a smart thermostat may learn the daily routine of a household and adjust temperatures automatically, maximising comfort and energy efficiency. Similarly, voice assistants integrated with machine learning can understand natural language commands, providing seamless control over multiple devices.

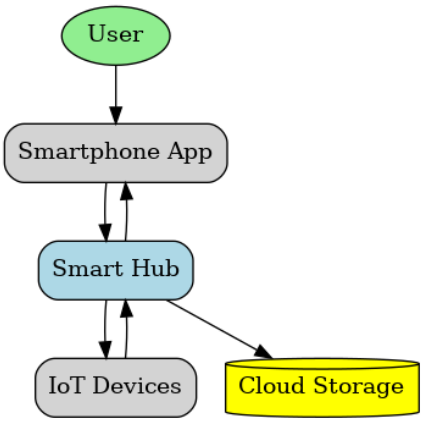


Fig 1. Shows a Data Flow Diagram.

This shows how data flows through the network connecting the User to their devices.

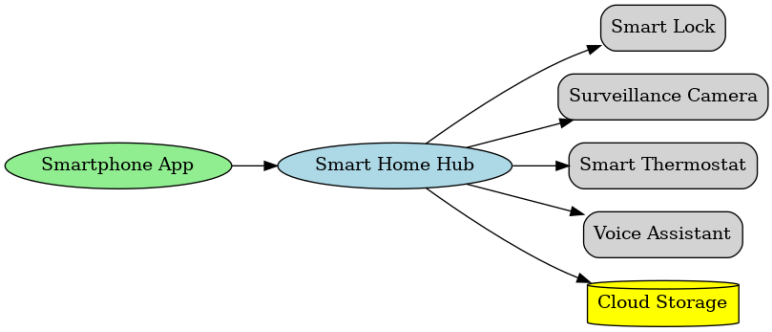


Fig 2. Shows a network diagram.

The network Diagram shows what devices are connected to the smart hub. The hub gives the user direct access to all the IoT devices.

# Analysis and discussion

## Attacking Methods

Smart homes face numerous critical security challenges. Many IoT devices lack robust encryption due to their lack of physical input and the need for configuration from a separate or centralized device. This necessitates active password changes, which users often neglect, creating vulnerabilities in their networks. (Velmurugan, et al., 2023). Furthermore, wireless networks pose a significant challenge. The absence of a physical connection allows anyone to discover and exploit vulnerabilities in these networks. (Touqeer, et al., 2021)

Some researchers have found that certain smart locks could be vulnerable due to flaws in communication between the lock and the app that controls it. For example, in one instance that involved a KeyWe Smart Lock, the encryption used when communicating between the lock and the app was weak. Skilled Attackers could intercept the Bluetooth signal and decrypt the signal, giving them access to the lock. This could allow a criminal to unlock the door when the owner is not around. (Townsend, 2019)

Smart cameras are also often targeted by hackers who aim to exploit weak security measures such as poor password management or unencrypted communication channels. In some cases, attackers can use scanning tools to find unsecured cameras that are accessible through the internet. Once accessed, these devices can be used to monitor and even manipulate the home environment without the owner's knowledge (Estopace, 2019)

When it comes to machine learning, hackers are using newer technologies such as artificial intelligence to develop new methods of exploiting smart devices. For example, a hacker may use AI to crack passwords, analyse network vulnerabilities, or develop malware that is specifically tailored to smart home devices. This trend highlights how technological advances can be a double-edged sword, helping both defenders and attackers in cybersecurity. (Gupta, et al., 2023)

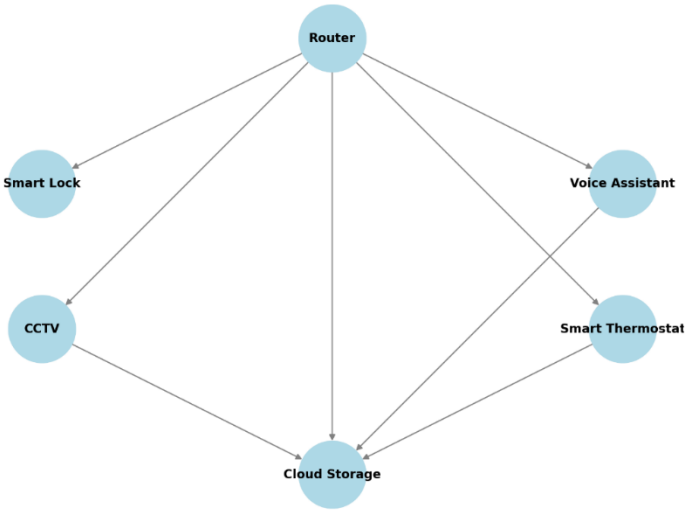


Fig 3. An attack graph. This shows the path an attacker can take to access devices on a smart home network

## Defending Methods

Defending a cyber-attack requires multiple levels of security, one such example is encryption. Encryption is a strong necessity to defend against cyber-attacks, encrypting devices with a secure password will prevent many attacks from low skilled hackers. Certain encryption methods are also crucial for cloud connected devices such as TLS or WPA3 for wireless communications. Without such robust encryption, attackers are able to intercept and manipulate data that is transferred on a wireless network, this would prevent attacks on vulnerabilities like the KeyWe Smart Lock attack (Townsend, 2019)

Furthermore, authentication is an extra step that can be taken to ensure that devices are secure, multi-factor authentication (MFA) should be used across devices especially when a smart home can be access remotely. MFA usually is a code that is either available in an offline off such as Google auth or that can be received over SMS. In newer cases MFA is available as a passkey stored locally on a device so a specific phone or laptop is needed to access the account or a passkey that is a physical device that needed to be plugged into the device logging in. MFA ensures that the person who is signing into an account or device is who they say they are. This also ensures that if a password is compromised there is still an extra layer of defence that will be needed to physically available to gain access to the account. (Touqeer, et al., 2021)

Machine learning can be used as an advantage, Machine Learning and AI can be trained to detect subtle attacks in systems by training itself on attacks and the system it is protecting. Then any changes that occur can be detected and delt with quickly, this can reduce the dependency for human interaction and the need to constantly monitor that the systems are running correctly and have no security issues. (Xiao, et al., 2018)

To go further with defensive on a network, Smart home devices can be segmented into separate virtual networks called VLANS. A VLAN separates up a network into many sub networks that all have different devices connected, they exist on their own local network but are still able to communicate with the other networks and the outside world. Having a VLAN setup like these where smart locks, security cameras and IoT alarm systems can prevent attackers from being able to move laterally through a network if a specific area of the network gets compromised. Slowing or even stopping a hacker greatly secures a network. (Rouiller, 2003)

# Conclusion

To conclude, smart homes can give security and control to the masses with their easy to setup, use and maintain devices that are able to be access to the general consumer rather than the need to install dedicated devices, however this ease can come at the cost of security. Smart devices can be subject to unsecure network access or weak passwords which can make them vulnerable to hackers hoping to gain access to a user's data or even potentially their home if they are able to hack a smart lock or alarm system.

Attackers are as always leveraging new ways to gain access to victims to data and machine learning and AI only makes the need for secure devices more necessary. Legislative advancements, such as the UK's 2024 laws mandating unique passwords and clearer security standards, are a big step forward in protecting the general consumer. Additionally, practical measures such as encryption, multi-factor authentication, and proactive security updates can significantly enhance the resilience of smart homes.

Ultimately, the security of smart homes depends on a collaborative effort involving manufacturers, policymakers, and users. By integrating robust defence mechanisms, enforcing stricter regulations, and educating user awareness, it is possible to reduce risks while maximising the benefits of smart home technology. The challenge lies in staying one step ahead in this ever-evolving landscape of cybersecurity.

# Team Contribution

Jake Cunningham 001211278

The work was completed in its entirety by Jake Cunningham, this includes the Research, Attack, and defence arguments as well as the diagrams.

# References


Estopace, E., 2019. *Smart homes under attack: security cameras, smart hubs most vulnerable — research*. [Online]
Available at: https://futureiot.tech/smart-homes-under-attack-security-cameras-smart-hubs-most-vulnerable-research/
[Accessed 11 2024].

Gupta, M. et al., 2023. *From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy,* Cookvillie, TN: IEEE.

Hill, K., 2013. *When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet*. [Online]
Available at: https://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/
[Accessed 10 2024].

Hooker, L., 2024. *Smart gadgets: Tougher rules for sellers of internet-enabled devices in the UK*. [Online]
Available at: https://www.bbc.co.uk/news/business-68917837
[Accessed 10 2024].

Rouiller, S. A., 2003. Virtual LAN Security: weaknesses and countermeasures. *GIAC Security Essentials Practical Assignment,* Issue 1.4b.

Touqeer, H. et al., 2021. Smart home security: challenges, issues and solutions at different IoT layers. *J Supercomput,* Volume 77, pp. 14053-14089.

Townsend, K., 2019. *Vulnerability Allows Hackers to Unlock Smart Home Door Locks*. [Online]
Available at: https://www.securityweek.com/vulnerability-allows-hackers-unlock-smart-home-door-locks/
[Accessed 11 2024].

Valencia, L. J., 2024. *2024. Artificial Intelligence as the New Hacker: Developing Agents for Offensive Security,* Socorro, New Mexico: New Mexico Institute of Mining and Technology.

Velmurugan, P., Senthil kumar, K., Sridhar, S. S. & Gotham, E., 2023. An advanced and effective encryption methodology used for modern IoT security. *Materials Today: Proceedings,* 81(2), pp. 389-394.

Xiao, L., Wan, X., Zhang, Y. & wu, D., 2018. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. *IEEE Signal Processing Magazine,* 35(5), pp. 41-49.