*algorithms*

MDPI

*Article*

# P3CRID: A Threat Model Methodology for Smart Homes

**Shruti Kulkarni, Alexios Mylonas * and Stilianos Vidalis**

Cybersecurity and Computing Research Group, School of Physics, Engineering and Computer Science (SPECS), University of Hertfordshire, College Lane, Hatfield AL10 9AB, UK; s.s.kulkarni@herts.ac.uk (S.K.); s.vidalis@herts.ac.uk (S.V.)

* Correspondence: a.mylonas@herts.ac.uk

**Abstract**

Threat modelling is a methodology employed for identifying and analysing threats and applicable mitigations for web applications, mobile applications, infrastructure, and environments including smart home environments. Threat modelling starts with a tabletop exercise to identify threats. It provides extremely important insights into what can go wrong if certain events or a series of events take place. The identification of these events is critical to ensuring the right mitigation strategies are applied. Threat modelling also helps to identify security controls that may be assumed to provide required security, but, in reality, may not be addressing the existing and applicable threat(s). Existing literature, in the public domain and in academia, discusses threat materialisation for smart homes; however, entry points for a threat to materialise and exploit these vulnerabilities are not explored and a dedicated threat model for smart home environments is currently unavailable. Whilst threats can be mitigated by smart home device manufacturers, there are also mitigations that need to be applied by smart home owners who are both technology-aware and technology-unaware. In this paper, we propose a structured, domain-specific threat modelling methodology for smart home environments. The methodology models threats from a smart home owner's perspective, identifies entry points and the mitigations that need to be implemented by a smart home owner. It also acknowledges that the attack surface expands and contracts and is not constant; which is addressed by applying zero-trust principles.

**Keywords:** threat modelling; attack vectors; mitigations; zero-trust policies; smart home environments

## 1. Introduction

The use of smart homes is on the rise because of the seamless automation and control, remote monitoring and access, and safety and personalised experiences they provide. In one of their reports, the UK Government mentioned that each home in the UK has an average of nine connected devices, and by 2050, the world will have 24 billion interconnected devices [1]. Interconnection in smart homes is brought about by voice assistants, home automation hubs, integrations, smartphones and so on. Now, devices can be instructed to perform an activity using a chain of devices, thus amplifying the attack surface [2]. A smart home owner can instruct a voice assistant to turn on a CCTV camera, which in turn switches on a smart light and supports motion detection with a motion sensor. Compromise of any of the devices in the chain of interconnections may result in lateral movement within the connected devices. This situation, when coupled with the fact that owners of connected devices can either be technology-aware or technology-unaware [3,4], results in differing



Academic Editors: Sihai Tang and Song Fu

Received: 10 February 2026
Revised: 2 April 2026
Accepted: 14 April 2026
Published: 1 May 2026

impacts of any threat materialisation as a technology-aware owner may secure the devices in a different manner than a technology-unaware owner.

Smart homes are different from a corporate or an industrial environment because smart homes do not have any formal organisational security policies and are not governed by any information security regulations or compliance requirements. As a result, smart home owners cannot be mandated to monitor their homes for vulnerabilities and to patch devices. The cycle of patching is also at the discretion of the owners, which often comes with a financial cost, such as upgrading a Jelly Bean operating system to an Oreo operating system, that the owner may not be inclined to incur. Similarly upgrading devices or adapting to new features may result in a learning curve, which, again, an owner may not be inclined to undertake. Senior people may not be very keen to learn about new features or about patching their devices. Smart home devices are manufactured by vendors who may or may not add security controls depending on the speed-to-market requirements. This in turn leads to the purchase of devices—with and without security controls—by smart home owners from common marketplaces or directly from the vendors. Lack of appreciation of the absence of security controls on the devices may result in adverse impacts on the smart home owners. In the face of such nuances, coupled with the need to secure smart home devices, it is important that smart home owners are provided with methodologies that help them identify threats and identify mitigations that are user-friendly for a smart home owner to implement.

We propose a structured threat modelling methodology for smart home environments, as the currently available methodologies are not entirely applicable to smart home environments when viewed from a smart home owner's perspective. Our threat modelling methodology is from the perspective of a smart home owner and not from that of a cloud provider or a mobile application developer. From a smart home owner's perspective, our threat modelling methodology answers two questions: a) Can anything go wrong in a smart home environment? And b) can any mitigations be applied by a smart home owner to reduce the risk of device compromises?

As such, our paper makes the following contributions:

1. We introduce P3CRID, a threat modelling methodology, which specifically targets smart home environments. To the best of our knowledge, we are the first to provide a structured, domain-specific methodology for this environment. We have applied the threat modelling methodology to use cases and created a threat model along with mitigations that can be applied by a smart home owner.
2. Due to the dynamic nature of the threat landscape, we list and regularly update the identified mitigations along with zero-trust policies on a GitHub repository (https://github.com/Shruti-s-kulkarni/smart-home-mitigations-P3CRID). Smart home owners can access this repository to help them understand the security implications of the threats, as well as the mitigations and zero-trust policies needed to address the threats.
3. We present the evaluation results for P3CRID, which are obtained via structured interviews with industry professionals.

The rest of the paper is structured as follows: Section 2 provides a background to threat modelling methodologies and related work. Section 3 contains the design of P3CRID and the implementation of two use cases. Section 4 evaluates the methodology. Section 5 discusses ongoing issues, limitations and directions for future work, before the paper concludes in Section 6.

https://doi.org/10.3390/a19050347

## 2. Background

### *2.1. Smart Home Environments*

A smart home environment is made of several smart devices, including but not limited to smart boilers, smart meters, smart televisions, smart bulbs, smart switches, integrations [5], and home automations. Smart homes are used and managed by both technology-aware users and technology-unaware users [3]. The authors of [4] discuss users' lack of understanding of security regarding smart home devices, irrespective of whether they are technology-aware or technology-unaware. This lack of understanding of security controls has security implications which are explored in this section.

The threats for smart home devices are different to the threats for IT, OT or industrial IoT devices. This is because all smart home devices are typically available on a single LAN, as demonstrated by [6], and when examined as an example architecture by ETSI [7]. In the absence of a guest network being enabled on the home router [6], any intrusion into a device may result in lateral movement to other devices, with few barriers. Nonetheless, depending on security awareness, a technology-aware smart home owner may have a choice to use more than one router to create a segmented network. However, this would result in more expenses as the owner would need to pay for more than one Internet Service Provider. Many users may not choose to incur this expense or may lack the technical expertise to do so. Irrespective of the number of home routers used, smart home devices depend on the home router for access control, stopping any malicious traffic coming in or any outbound internet connections being made with malicious IP addresses or malicious external cloud storage. Unlike IT, OT, IoT or industrial IoT environments, it is difficult to capture egress traffic from smart home devices, as owners may typically not choose to use Intrusion Detection System/Intrusion Prevention System (IDS/IPS).

Updates and patching smart home devices are challenging as they may have a financial impact. Asking users to upgrade their device to remediate a vulnerability may result in an expensive purchase, which the owner may not want to incur [8]. Applying over-the-air software patches of smart home devices may be challenging, as a smart home owner may ignore the patching notifications or may choose to postpone the activity.

Smart home environments do not have any overarching information security policy management system or any applicable regulatory/compliance requirements, such as ISO27001 [9]. Information security policy management systems apply (if mandated by a regulatory authority or legal requirements) to vendors who manufacture the devices. The owners cannot be compelled to follow them. Owners of smart televisions, smart bulbs, smart switches and so on cannot be compelled to follow policies such as vulnerability management and patching policies.

The devices are manufactured by diverse manufacturers who have varying maturity levels of security standards. It may be challenging to enforce common security standards among vendors unless there are protocols such as Matter, which enforces security on devices that are certified by the Connectivity Standards Alliance [10] or by enforcing ETSI standard [7]. Detecting any security incidents that may materialise in a smart home environment is difficult because of the absence of logs and monitoring, as well as a lack of security controls that can detect anomalies, unless a smart home owner chooses to detect anomalies, which would be an exception and not a common practice.

In the face of such disparities in the security controls of smart home devices, a lack of security policies/regulatory requirements and a varying range of technical skills, a smart home environment needs a solution that supports the security of the devices which can be implemented by smart home owners with the necessary technical expertise and those without. The solution also needs to reduce cognitive burden such that the security of smart homes is appreciated and implemented by smart home owners.

### *2.2. Threat Modelling Methodologies*

Threats are prevalent for assets and information that have value or can be weaponized. Information like personally identifiable information (PII) has value because if PII is acquired maliciously, a malicious actor can steal the identity of the person [11]. Conversely, information that can lead to security decisions for a device, such as making changes to the configuration of vital services, can be weaponized to impact the public or individuals at large. Reports from [12] show how home technology can be used to abuse victims. A widely known example of the weaponisation of public-related data is the attack on citizens of a small town in Pinellas County, FL, USA. The attack was prevented by a water treatment plant operator who noticed the attackers increasing the levels of sodium hydroxide in the water supply to a dangerously high level [13]. Assets are impacted with a loss when a threat materialises to exploit a vulnerability.

This paper does not delve into the details of how the loss is calculated. It will, however, list threats, vulnerabilities and the resulting impact of risk materialisation for smart home devices which act as assets for a smart home environment. Risks need to be treated before threats materialise. Risks are managed in four ways: (a) by accepting the risk, (b) by avoiding the risk, (c) by transferring or sharing the risk and (d) by mitigating the risk [14].

To treat risks, the applicable threats, applicable vulnerabilities, assets in scope and impacts of risk materialisation must be identified. A threat model is a structured representation of threats applicable to assets/information and corresponding mitigations designed to protect information/assets of value [15,16]. Various environment agnostic threat model methodologies are available to perform a threat model [17], including, but not limited to, the following: STRIDE [18], VAST [19], PASTA [20], TRIKE [21], LINDDUN [22], and OCTAVE [23].

STRIDE identifies threats using the expansion Spoofing, Tampering, Repudiation, Information Disclosure, denial of service and Elevation. In practice, it is widely used to threat model APIs and applications, both web and mobile. The main purpose of the STRIDE threat model method is to apply the model to cyber and cyber–physical systems that are a part of the same ecosystem. Research in the public domain and in academia acknowledge that STRIDE is for software development and is not suitable for other domains or industries [24,25]. Threats like spoofing may avoid the abuse of identities and only focus on the spoofing of identities [24].

PASTA identifies threats using the Process for Attack Simulation and Threat Analysis, which combines business context with technical analysis to identify threats to organisations and applications. The creators of the method acknowledge the fact that PASTA helps organisations prioritise the security of their assets while working to minimise risks and impacts. It helps the involved stakeholders to assess threats and develop effective risk mitigation strategies. However, smart home devices (smart home assets) have equal priority as they are typically on a single VLAN [7].

VAST is an acronym for Visual, Agile, and Simple Threat modelling and is focused on identifying threats to vulnerabilities of enterprise applications and IT systems. VAST relies on automation and not on manual methods of identifying threats. It relies on operational tools; it is agile and brings an iterative approach to the software development lifecycle. As the method's focus is on the software development lifecycle, it is challenging to use VAST to threat model smart home environments.

The Trike threat model method focuses on data flows and important stakeholder assets. Trike is a useful method for the risk management of assets from a perspective of identifying defensive controls. Trike is also useful when creating an access control matrix that defines the create/read/update/delete (CRUD) permissions for the actors to perform on IT assets. For smart home environments, though create/read/update/delete

permissions exist, they are typically carried out by device manufacturers. For home automation systems, permissions applied by the owner are for the devices to make changes and not for actors to make changes. The threats for a smart home environment go beyond the access control matrix, making Trike unsuitable.

LINDDUN (i.e., Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness, and Non-compliance) is a privacy threat modelling framework. The method requires the analyst using LINDDUN to have extensive privacy expertise and experience in threat modelling. Smart home owners may not have the level of expertise required to use LINDDUN. Like Trike, LINDDUN also looks at data flow diagrams and considers asset categories such as computational units, data stores and external entities. The method does not consider security threats such as malware being pushed into a smart home device via an approved HTTPs connection between the cloud and the device, leading to gaps in threats identified for smart home environments.

OCTAVE (i.e., Operationally Critical Threat, Asset, and Vulnerability Evaluation) is aimed at identifying operationally critical threats. The methodology considers three types of assets: assets that hold information (i.e., health information, intellectual property), infrastructure assets (i.e., servers, network equipment) and human assets. OCTAVE assumes that the employees of the organisation in question possess institutional knowledge; hence, it is best to threat model the organisation from an operational perspective. It has a dual focus, blending both technical and business perspectives, making it unsuitable for a smart home because of the missing business perspective.

The methodologies discussed above do not completely address the threats affecting smart homes that are influenced by various background nuances specific to a smart home environment. A comparative analysis of the environment agnostic methodologies is presented in Table 1. P3CRID addresses the gaps in the existing threat models.

**Table 1.** Comparative analysis of applicability of environment agnostic threat modelling methodologies to smart home environments.

| Threat Model | Main Domains | Strengths | Limitations |
| --- | --- | --- | --- |
| STRIDE | APIs and applications (web and mobile). Cyber and cyber–physical systems within the same ecosystem. | Applicability to software. | Misses threats such as lack of technology awareness, lack of information security policies. |
| PASTA | Combines business context with technical analysis to identify threats specific to organisations. | Prioritises assets, assesses threats, and develops mitigation strategies. | Misses environments with devices of equal priority that are hosted on the same VLAN. |
| VAST | Enterprise applications and IT systems using automated tools. | Agile and iterative. Integrates with the software development lifecycle and automation tools. | Misses threats such as lack of technology awareness, lack of information security policies. |
| Trike | Defining defensive controls using access control matrices. | Useful for defining and analysing access control and permissions. | Misses threats such as open ports, supply chain risks and machine identities. |
| LINDDUN | Privacy-focused threat modelling framework. | Strong focus on privacy threats and privacy-by-design principles. | Misses threats such as malware delivered through legitimate cloud device communication. |
| OCTAVE | Identifies critical threats (for operations) across information, infrastructure, and human assets. | Combines technical and business perspectives for risk assessment. | Misses threats for environments that do not have prevailing business perspectives. |

### 2.3. Attack Surface and Communication Vectors

Extracting common denominators from the technical reports and papers [7,26–35] the layered stack of smart home devices consists of the following: (a) hardware, (b) firmware/OS, and (c) network. Smart home devices typically have a cloud environment, a mobile application, an optional web application and optional integrations. The network protocols appearing in Figure 1 are indicative communication vectors curated from (a) a matter database [36], including devices that have the capabilities of Thread, Wi-Fi and Bluetooth-connected Matter devices, and (b) a Vesternet database that offers z-wave and ZigBee devices for sale [37–39].

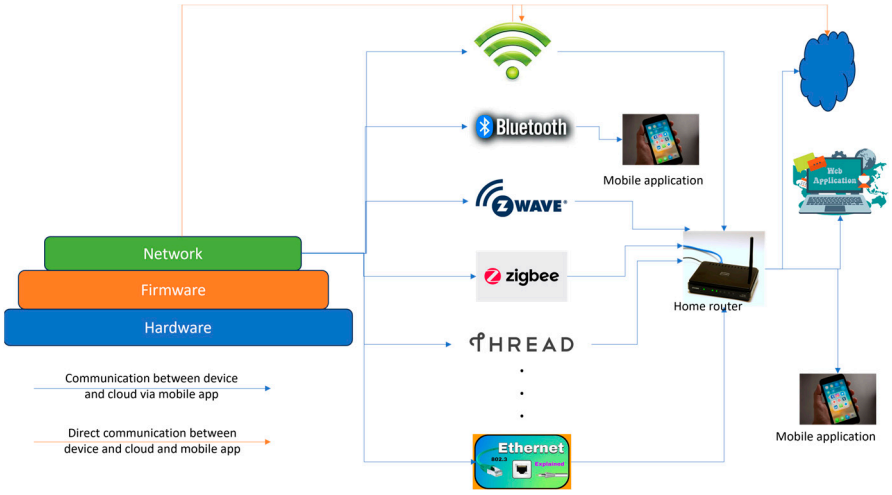


**Figure 1.** Technology stack of a smart home device.

The authors of [4] have elaborated on the attack surface for an example smart home environment, as depicted in Figure 2.

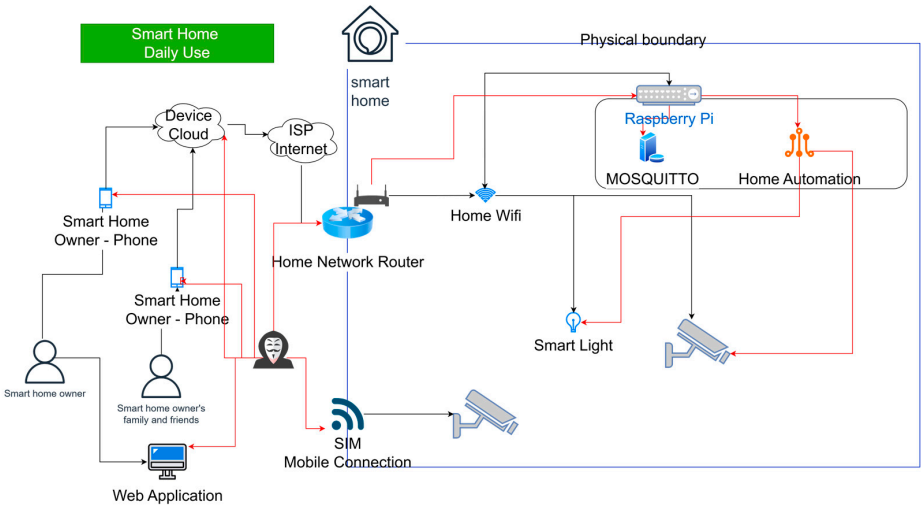


**Figure 2.** An example of a smart home environment [4].

The authors [4] indicate that the attack surface for a smart home environment includes (a) the smart home devices themselves, (b) cloud environments, (c) mobile applications, (d) web applications, (e) integrations with home automations, (f) communication lines, (g) network protocols used in communication with smart devices, and (h) home routers. However, with integrations [40], the smart home environments now include assets such as a MQTT server, and a web server, thus increasing the attack surface. Integrations are depicted

in Figure 2. The ease of using integrations with smart home devices is demonstrated in both academia [41] and the public domain [5,42,43].

An example of such integrations in a smart home environment can be seen in Figure 3.

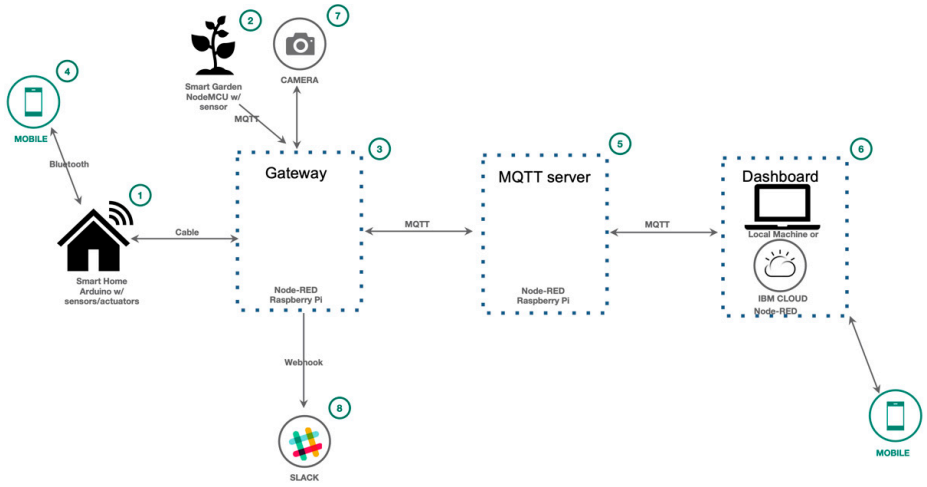


**Figure 3.** An example of a smart home environment, with integrations [41].

An increase in attack surface is also due to cellular-enabled smart home devices [44,45] as these devices have public IP addresses. Assets are the main components of and make up a smart home environment [46]. Asset categories also include near-field activated devices.

Communication vectors are also part of the attack surface for smart home IoT systems; they encompass many interconnected devices and communication protocols vulnerable to unauthorised access or exploitation [47]. Passive traffic sniffing meant to compromise the transport layer typically requires that the attacker has local network access, either by being on the same LAN/Wi-Fi segment or by compromising an intermediate network component, such as a router or access point (passive sniffing is inherently local network-bound) [48]. As a result, passive network listening is not considered a remote threat vector for data exfiltration or exposure in typical smart home deployments, assuming the use of standard network isolation and encrypted transport protocols [49].

The attack surface for a smart home environment expands and contracts based on the devices used, the integrations implemented and the remote connections put in place. After factoring in the technical skills of the users and the ease of setting the integrations and remote connections, it is challenging to keep up with the security controls required to secure the devices. This anomalous situation needs to be addressed with dual controls: securing the devices and securing the use of the devices. Securing devices from threats is the duty of the vendor, as a smart home owner would purchase a device and not build one. However, securing the use of the devices from threats can be addressed by smart home owners if they have access to the right level of advice, education and training [46,50].

A threat is a circumstance or an event that can potentially impact an entity adversely [51]. The entity could be an organisation or an asset or an environment. In addition, an attack vector [52–54] is a route adopted by a threat actor to carry out malicious activities on a system or an asset, for a gain or to create disruption. An attack vector is also referred to as a threat vector. A threat actor [55] instigates the threat, either by discovering a vulnerability or by actively seeking to discover a vulnerability in order to cause an impact.

In particular, the available attack vectors for a smart home matched to MITRE ATT&CK [56], include (a) physical access, because cyber-enabled physical access devices (such as smart lock devices) with weak SSID credentials, vulnerabilities, etc., can lead to compromised physical barriers of smart homes; (b) cloud environment, because misconfigurations or malicious insiders in the cloud environment can lead to unauthorised

access to smart home owners' cloud-stored data; (c) applications, mobile and/or web, because compromised vulnerabilities in the application or an absence of MFA on the web application can result in changes in the settings of the smart home device(s); (d) home routers with which any insecure ports enabled on the router could allow second-order attacks; (e) integrations with which malicious commands can be processed, malicious emails or calendar invites can be read, leading to damage of the devices or emotional impacts due to rapid configuration changes; (f) supply chain, because devices can be assembled using third-party components with vulnerabilities; and (g) cellular devices, because their public IP addresses are discoverable and could be compromised with their accompanying administration consoles that may contain vulnerabilities [57].

Vulnerability [58] or weakness [59] is a deficiency in a system or an entity that may lead to undesirable effects when a threat materialises. Using the route of attack vectors, a threat actor compromises vulnerabilities in the assets to reach the assets. Vulnerabilities related to smart home environments have been curated from open-source vulnerability databases such as Vuldb.com [57], exploit-db [60], and Censys.com [61]. The following is a curated list of vulnerabilities related to smart home devices:

(a) A lack of security processes, leading to (i) ineffective authentication and access controls, weak credentials or over-permissioned identities which can be brute forced; (ii) a lack of logging and monitoring procedures, leading to lack of visibility to incidents; and (iii) a lack of firewall rule reviews, leading to over-permissioned firewall rules.

(b) Security misconfiguration or weak configuration, leading to (i) incorrect or missed system hardening, (ii) weak cryptography cyphers, (iii) databases exposed to the internet, (iv) databases without any authentication procedures, (v) ease of opening ports on firewall/router, (vi) open insecure ports on firewall/router, (vii) a lack of approval for the automated opening of ports such as uPnP.

(c) Lack of secure coding in applications leading to (i) cross-site-scripting, (ii) cross-origin resource sharing, and (iii) man-in-the-middle attacks when public keys are not pinned.

(d) A lack of security testing leads to undiscovered and untested vulnerabilities in applications that can be exploited by malicious actors.

(e) A malicious supply chain manifests vulnerabilities in various ways, through (i) backdoors in firmware and hardware as well as (ii) built-in malicious code.

(f) Lack of security awareness leads to (i) the insecure use of devices and services, such as clicking on a link in a phishing email or not suspecting a social engineering attack, which in turn can lead to AI prompt injection on voice assistants, (ii) building insecure applications for both web and mobile applications and (iii) building insecure devices with a lack of supply chain assessments.

(g) Lack of security features leads to (i) the insecure use of devices, leading to a lack of mitigation regarding prevalent threats, such as not encrypting data in transit, (ii) not encrypting data at rest, (iii) storing credentials in clear text, and (iv) a lack of secure management of keys.

Impacts include the harm that is caused when a threat actor uses an attack vector to trigger a threat and exploit a vulnerability [62].

For a threat to materialise and cause an impact, the asset and its associated vulnerability(ies) must be visible to the threat actor in order for them to exploit it. Extending this definition to smart homes, in order to compromise a smart home environment, an external threat actor needs visibility of the attack surface and the vulnerabilities it may have. This act of gaining visibility to the attack surface and its vulnerabilities is referred to as reconnaissance on MITRE ATT&CK [56].

There are two reconnaissance for the attack surfaces of smart home environments, namely: (a) the one that has devices with public IP addresses and (b) near-field con-

nections, such as Bluetooth and RFID. Smart home devices that are not on a cellular network are not visible on public networks/internet on their own. This is because the devices do not have public IP addresses. They are on the internal LAN/VLAN with private IP addresses; network address translation (NAT) is typically provided by the home router [36,63–65]. Devices with private IP addresses are not visible to threat actors using a public network/internet connection.

Circling back to reconnaissance for smart home environments, as discussed in Section 2, connections to smart home devices can exist with near-field network protocols, such as Bluetooth and Thread. For instance, Bluetooth connections are discoverable by a threat actor who is within a distance of 43 metres (10 metres on an iPhone) [66,67], in contrast with a threat actor who is on a public network and can discover other entry points into a smart home with technical components, including (a) clouds, (b) mobile applications, (c) web applications, (d) home routers, (e) externally exposed integrations, (f) supply chain risk materialisation on smart home devices, and (g) breaking the physical barrier. Any externally visible vulnerabilities in these components can be discovered remotely by a threat actor, which in turn are used to access smart home devices via existing/discoverable attack vectors or entry points. Reconnaissance for smart home environments now expands beyond devices with public IP addresses and Bluetooth connections.

Our research provides a collection of matching security controls for a smart home owner to apply based on their applicable threats. These security controls are mapped to zero-trust policies by looking at each device as a protect surface and not as an attack surface, which helps to identify mitigations when more devices are added or a new network protocol is introduced.

The rest of the section focuses on the threats that are applicable to smart home environments.

#### 2.3.1. Physical Perimeter Threats

Smart home environments can be subject to cyber–physical attacks [50]. For instance, a smart lock can be bypassed [8] and could allow malicious actors to enter a home and cause bodily harm, or lead to burglary. Malicious profiling or occupancy detection can lead to burglary or stalking. Authors [68] discuss the cyber-enabled harm caused by smart home devices, including fraud, stalking and grooming. These harms could be carried out by (a) obtaining unauthorised access to systems (activation of web cam, control of voice-assisted devices), (b) malicious changes to security settings, and (c) damaging devices to ensure that the security functionality is not available, including compromised door locks, burglar alarms, and CCTV cameras.

The authors of [46,69] discuss malicious actors entering homes of vulnerable people/technology-unaware owners and changing security controls. Furthermore, smart locks running on ZigBee, z-wave, and Bluetooth can be jammed and disabled, as demonstrated by [8]. Such attacks can help the attacker bypass the security offered by the devices and/or cause a denial of service for the users.

The author of [70] discusses two types of locks that use similar types of keys: passcodes, PINs, fingerprints, RFID smart cards, and mobile apps that control locks via Wi-Fi and low-energy Bluetooth. The keys can be compromised with cloned cards (for example, Flipper [71]), bluesmacking, bluejacking, bluesnarfing, and KRACK attacks on the WPA2 protocol (which allows an attacker to copy and keep the keys forever).

The authors of [72] discuss smart locks that contained vulnerabilities, especially the presence of dangerous permissions or a lack of required permissions. They also discuss the vulnerabilities in applications supporting the smart locks and the impacts of exploiting such vulnerabilities on the physical safety of the smart home. Security controls exist on smart home devices such that appropriate settings may be enabled by the smart home

owners [73]. These settings could be either mis-handled or may be inadequate. For example, static keys that are required for the devices to communicate with its application may be discovered by a malicious actor.

Threat materialisation achieved via the covering of CCTV cameras installed outside of a smart home are known to take place, but evidence of this type of attack is not easily available in the public domain and in academia. Also, the risk of disconnecting the ethernet cable that runs from the Internet Service Provider's hub to the home's router—accidentally or deliberately—is difficult to prove. These actions cause a larger impact on an unoccupied house that is monitored with CCTV cameras and an internet connection that uses the ethernet cable.

Any retrieval of the SSID and the PSK of the Wi-Fi connection from the devices would result in the attacker virtually living in the smart home [74]. Smart home owners share passwords for the SSID of their Wi-Fi routers. The shared credentials are stored on their devices, which if stolen can lead to malicious connections into the smart homes [75].

Any SSID with a weak password may be brute-forced, giving attackers access to all smart home devices in the environment [76]. Similarly, a Bluetooth connection without any verification code can be accessed with [77].

Figure 4 shows the attack vectors that a malicious actor can use for threat materialisation via physical access.

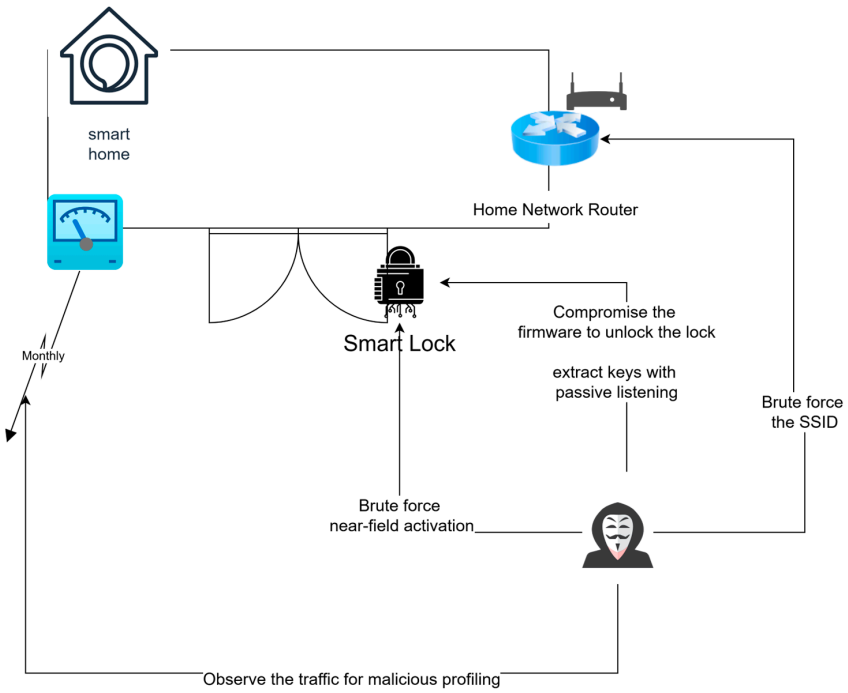


**Figure 4.** Materialisation of compromise of physical access.

### 2.3.2. Cloud-Related Threats

The authors of [78,79] discuss functionalities such as the control, monitoring and managing of smart devices via cloud connections. Smart home devices that connect to the cloud to also provide remote access for management of the devices, which includes switching off a smart bulb or monitoring CCTV feeds. Vulnerabilities in the cloud include a lack of security features for the components that make up the cloud, the absence of security processes in the cloud, a lack of security awareness from the personnel who maintain the cloud and weak configurations or security misconfigurations.

Any compromises in the cloud environment can lead to compromise of the data of smart home devices persisting in or shared via live feeds in the cloud environments.

Compromises can also take place via capabilities that inject components into smart home devices. Ref. [69] discusses ways in which physical access can be compromised via the cloud and applications. These methods include the following: (a) unencrypted backups exposing credentials or authentication data that are then used to compromise devices, allowing attackers to break into houses; (b) preventing sensors from detecting risks such as fire, motion, and carbon monoxide leaks by jamming and tampering at the physical layer; (c) malicious profiling with statuses of door locks and smart meter signals; and (d) determining occupancy with a compromised motion sensor. For example, from 8 to 9 March 2021, Verkada's cloud platform was compromised via a misconfigured customer support server that was exposed to the internet. The attackers accessed cameras and viewed video and image data [80].

Security researchers Noam Rotem and Ran Locar from vpnMentor discovered a user database belonging a company called Orvibo, which runs a smart home management platform. The database was available on public networks/internet without any password. The database stored more than 2 billion records containing everything from user passwords to account reset codes and even a "smart" camera-recorded conversation.

An organisation that managed clouds misconfigured an Elastic database and exposed it to a public network (with a public IP address) [77,81]. CCTV feeds that were sent to a cloud environment and CCTV images that accept direct feeds from CCTV cameras installed in smart homes [82] were compromised via compromise of the cloud.

As per documents dated June 2014, the operating system of Samsung smart televisions were designed to create a "fake-off" mode that made users believe the television had been switched off, when in fact recordings of conversations in the smart home were transferred to the destinated cloud once the televisions were switched back on [83,84].

Figure 5 shows the attack vectors that a malicious actor uses for threat materialisation of compromise via cloud.

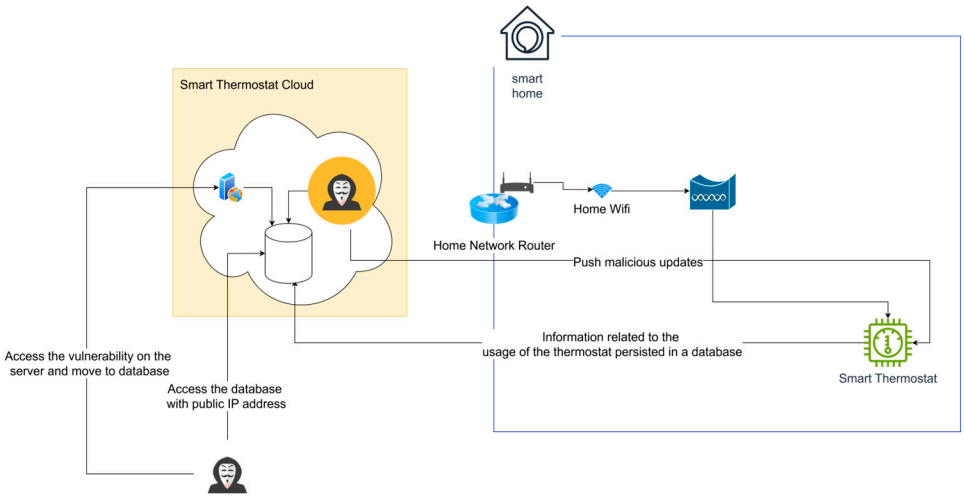


**Figure 5.** Threat materialisation of compromise via cloud.

### 2.3.3. Threats from Mobile Apps and Web Applications

Smart home environments are compromised when web applications and mobile applications are built insecurely due to lack of secure coding, which leads to vulnerabilities in the applications, a lack of security testing leading to a lack of knowledge of existing vulnerabilities in the applications and misconfigurations or weak configurations. As an attack vector, applications (mobile or web) could allow a malicious actor to make unauthorised changes to the device settings, move laterally using network protocols,

observe communication in clear text, cause denial of service for the smart devices, or connect to other smart devices via their vulnerabilities.

Applications (web and/or mobile) typically configure the smart devices and optionally monitor them. Modern smart home devices are configured with a mobile application using near-field activation methods such as Bluetooth. Attackers that compromise vulnerabilities in mobile apps then move on to compromise vulnerabilities in network protocols (ZigBee, z-wave, Bluetooth, Thread, matter). This is demonstrated by the authors of [85], who moved laterally in a smart home environment using smart light bulbs when mobile application exploited the non-mandatory use of asymmetric keys for authentication and authorization when using a ZigBee protocol. The author of article [86] describes how malware could be installed on a smart bulb that can then control the lights and the control hub.

The authors of [65] discussed the feasibility of malware in a mobile application to circumvent the firewall rules on a home router. The authors demonstrate that such malware can scan the smart home environment to locate smart devices in the home, identify vulnerabilities and expose the smart devices to public networks, thus defeating the very purpose of the internal network provided by the home router.

A security researcher disclosed cross-site scripting (XSS) in the web interface of Tasmota [87]. Separately, a different security researcher disclosed an HTTP CORS issue on the Tasmota web interface, mentioning that the vulnerability was complicated, along with the fact that the web application does not require a password [88].

Threat actors who compromise vulnerabilities in mobile devices like laptops, desktops, tablets, etc., move laterally in the environment to compromise other vulnerabilities in mobile apps and place malware in smart home devices or move laterally in the smart home environment, as discussed by [89,90]. The authors of [91,92] discuss the impact of cross-site scripting that is present on the web application of a smart home device. Brute force attacks on the mobile applications of smart locks are discussed by [93,94], where a malicious actor was able to open doors using unpatched applications.

Compromised smart home devices via web applications have been reported by [95,96]; a couple reported changes in thermostat temperatures and music coming from security cameras. This breach was attributed to the reuse of passwords on Nest and the absence of multi-factor authentication (MFA).

Figure 6 shows the attack vectors that a malicious actor uses for threat materialisation of compromise via mobile applications.

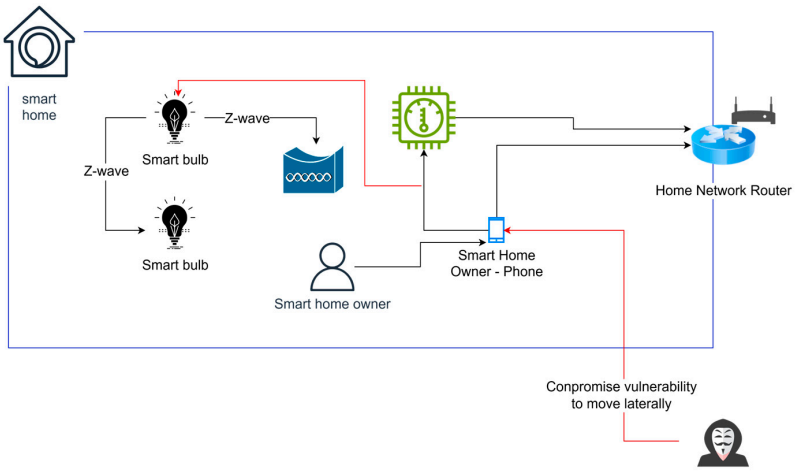


**Figure 6.** Materialisation of compromise via mobile applications.

Figure 7 shows the attack vectors that a malicious actor uses for threat compromise via web applications.

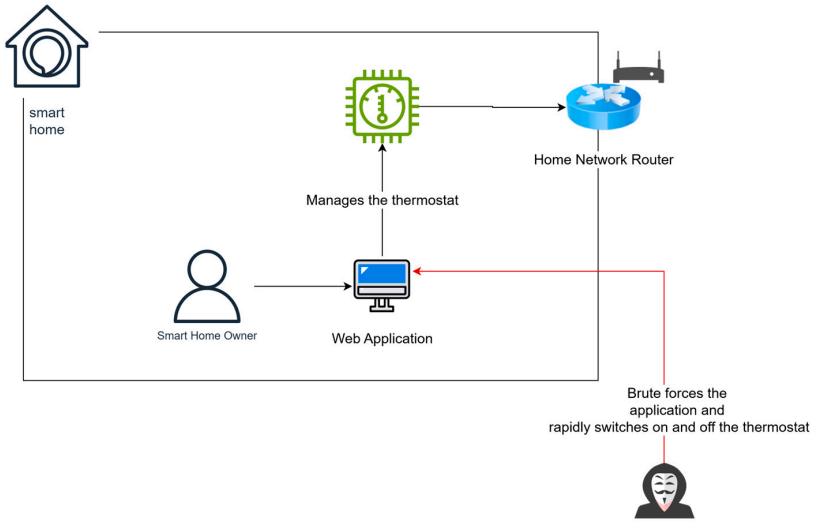


**Figure 7.** Threat materialisation of compromise via web application.

#### 2.3.4. Threats from Home Router

The threat of compromise via home routers is due to vulnerabilities such as a lack of security processes enforced by the manufacturers, a lack of security awareness or a lack of security testing, resulting in exposed ports, embedded credentials, default credentials, etc., [6]. As an attack vector, routers can be used to carry out further compromises and forward traffic to malicious destinations via port forwarding [6]. The absence of any configured policies on the router may enable smart home devices with capabilities to open ports on routers; for example, cameras opening ports on routers. Reports of routers permitting cameras to open ports without user consent have occurred in the distant past, but this is not a frequently appearing example [97] in recent times. However, exposed ports, weak passwords, default credentials, deprecated protocols, etc., that allow a malicious actor to access the router and scan for devices in the smart home environment have been demonstrated by various authors [6,97–99].

Home routers with weak policies may be passive participants in second-order attacks, as described by a security researcher who has written about compromised home routers attacking word press sites [100]. The report also includes traffic forwarded to malicious sites by compromised routers. These routers had ports 21, 20 and 25 open, among others, and they were subjected to eavesdropping [100,101]. Reports of more vulnerabilities with routers used in smart homes are demonstrated in [102–104].

Threat materialisation via compromise of routers is depicted below in Figure 8.

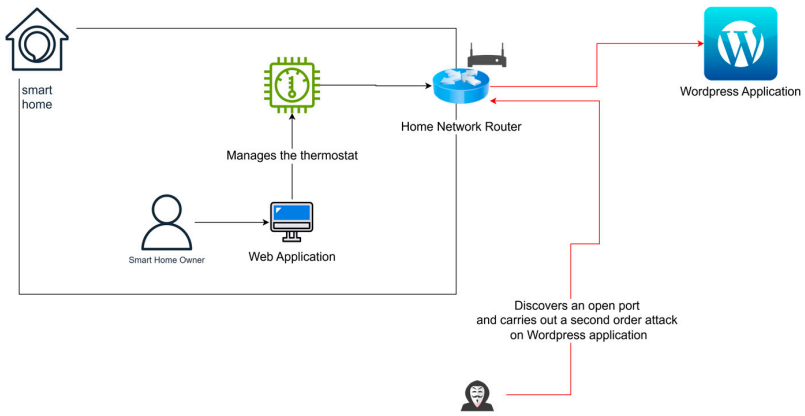


**Figure 8.** Materialisation of threat compromise via home router.

#### 2.3.5. Threats from Integrations

Smart home integrations connect various smart home devices to provide a unified, seamless experience for smart home owners. Currently, integrations are available as add-on components, such as voice assistant and virtual assistants, or they can be created from software programmes available on GitHub or can be built using discrete components like Mosquitto servers for communications using Message Queuing Telemetry Transport (MQTT). Integrations are attack vectors, as any compromise of vulnerabilities in the software programmes or home assistants or voice assistants can result in an impact. The vulnerabilities include a lack of secure coding, a lack of security testing, a lack of security processes followed by the owner, and a lack of security awareness by both the integration provider and the home owner.

Smart home integrations provide seamless automation and control, ease of use, convenience, personalization and accessibility. Depending on the functionality in place, integrations store credentials, which can be stored in clear text. Integrations such as MQTT or SBM blocks can be enabled to be visible on the internet. Compromised vulnerabilities in software applications could lead to lateral movements in smart home environments and control over devices [85]. Official documentation from a provider of home integration for home automation documents that user information (including device information, certificates, tokens, etc.) from the user's account is stored in clear text after successful login [105].

The Home Assistant, which provides local smart home control, disclosed a vulnerability [106] caused by a lack of authentication which allowed an attacker to access any file that was accessible by the Home Assistant process. This access included any credentials that might have been stored to allow the Home Assistant to access other services.

The Home Assistant disclosed a different vulnerability [107] which allowed an attacker to remotely bypass authentication and interact directly with the Supervisor API, called the Supervisor (the operating system of the Home Assistant). The attacker can then gain access to Home Assistant updates, add-ons and backups.

A finding by Avast, the world leader in digital security products, shows that more than 49,000 Message Queuing Telemetry Transport (MQTT) servers are publicly visible online worldwide due to protocol misconfiguration. In France, nearly 900 servers, unprotected by passwords, were found exposed, putting them at the risk of data leakage. On the hub software, communications are public and accessible to malicious actors if they are made via the open and unprotected Server Message Block (SMB) protocol, used to share resources on internal networks, primarily on Windows. Avast also found that directories are shared with all Home Assistant files, including those related to configuration. Among the exposed files, Avast identified one containing passwords and keys, stored in plain text. This information could allow an attacker to completely control a person's home [108].

The authors of [109] discussed side-channel attacks conducted by malicious applications using attacks such as timing analysis, simple power analysis, and differential power analysis. Such attacks are capable of malicious profiling, resulting in occupancy detection. Malicious profiling has been discussed by researchers [110] when they inferred user activities with high accuracy.

Security researchers from [111,112] report on and discuss the attack vectors used on Apple smartphones to infect speakers, which in turn infect other smartphones. Third-party AirPlay enabled devices that were allowed to run their own code on Apple products, acted as attack vectors. This resulted in third-party users connected to the same home router as a smart TV, speaker or set-top box at a party, to potentially use open AirPlay connections to spread malicious code from one device to another. Bluetooth-enabled integrations are used by threat actors for eavesdropping.

Researchers demonstrated control over smart home devices by using a poisoned Google calendar, in the form of an AI prompt [113]. The authors of [114,115] demonstrate several abuse cases of prompt-ware. The authors describe how a malicious calendar entry or an email that is accessed and read by the voice assistant can lead to a boiler being set to a boiling point, window blinds being opened, etc. The authors of [116] researched attacks on the web interface of smart devices, which led to brute force attacks on the devices.

Laser-based command injections of malicious commands on voice-controlled microphone arrays have been researched by [117]. Though laser signals cannot travel past walls, they can be used on open windows, especially unguarded windows that are left open at night.

Threat materialisation of compromise via integrations using attack vectors is depicted in Figure 9.

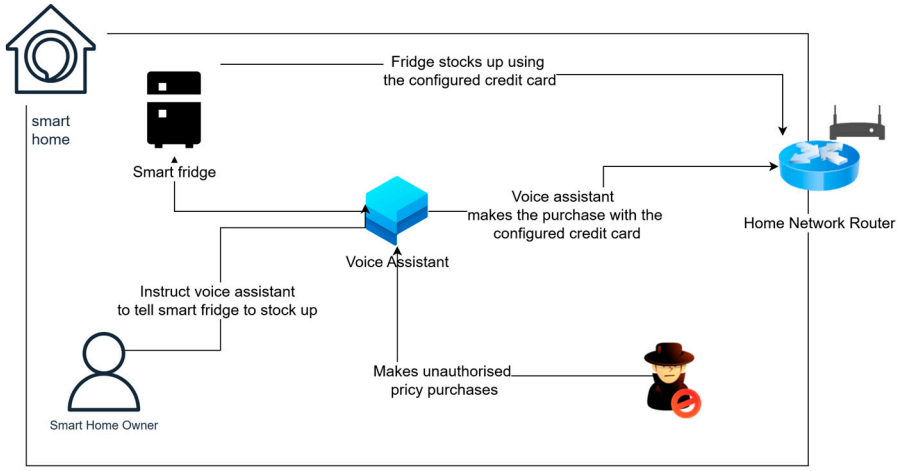


**Figure 9.** Threat materialisation of compromise via integrations.

### 2.3.6. Threats from Vulnerable Devices

Vendors adopt various ways to build smart home devices: a) they obtain components of the technology stack—hardware, firmware, network interface—as commercial off-the-shelf (COTS) products from third parties, assembling them together to build smart home devices; b) they outsource the assembly and/or build of the components to third parties; or c) build the entire device in a factory environment. In this paper, we will not describe the details about how the base-level components, like the various items of hardware (RAM or ROM that may be purchased from third parties) or firmware (third-party code available on GitHub), are assured for security by the manufacturer. This paper focuses on hardware and/or software and/or network components purchased from third parties by smart home vendors that are put together to manufacture the devices and ship them for sale.

Smart home devices are an attack vector that compromise vulnerabilities such as a lack of supply chain management, a lack of security processes, a lack of awareness and a lack of security testing, resulting in impacts on the smart home owner.

The authors of [118] discussed various supply chain-related threats for IOT devices, including smart home devices. They discuss device manufacturers and their reliance on commercial off-the-shelf (COTS) products; these provide them with various advantages, such as reductions in the cost of production and speed-to-market effects. This reliance brings about security issues, as a lack of security assurance for the procured components may lead to the shipping of devices with vulnerabilities.

Security researchers [86,119] discuss vulnerabilities in smart home devices (hardware, firmware, bridges). They discuss how, despite the lack of visibility of smart devices and their vulnerabilities on public networks/internet connections, compromised devices may

exploit existing vulnerabilities to send data to malicious locations because the egress communications are encrypted and outbound communications are not monitored.

Cybersecurity firm A&O IT Group Clear found vulnerabilities [120] in smart plugs, and one of them was that the plugs communicated over HTTP in place of HTTPs; this includes the SSID and the WPA2-PSK sent in clear text. This communication not only impacts smart plugs but also the whole of the smart home environment. A malicious actor capturing the PSK can position themselves in a nearby reachable location and enter the smart home environment, virtually.

Security researchers [121] discuss the impact of supply chain risks in smart doorbells and smart cameras and the privacy violations that take place because of such vulnerabilities. They discussed the compromise of sensitive information about the device's owners and how smart gadgets were taken over, for example, by speaking through the devices, stealing footage and recordings, or flickering the lights. Bigger companies can enforce fixes quickly when a vulnerability is disclosed. That is not always the case for smaller brands. Security breaches impact companies of all sizes. Amazon and Google have experienced security breaches with Ring and Nest security devices in recent years.

Devices that connect to clouds that are in a jurisdiction with different privacy rights for citizens compared to the area where the consumers are located, pose privacy issues for consumers [122]. Any threat materialisation with such devices results in privacy violations for the owners and could also lead to espionage of people of interest and high-profile individuals.

Figure 10 shows an instance of a malicious actor using attack vectors to materialise threat compromise via vulnerable devices.

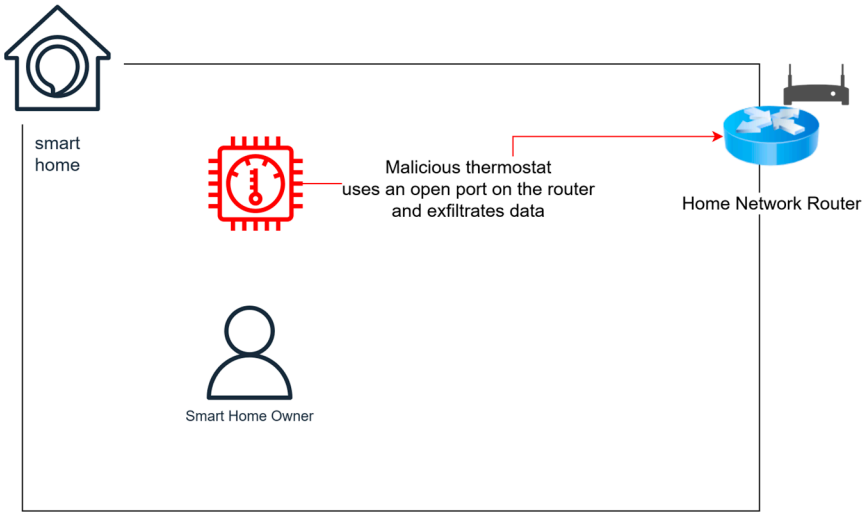


**Figure 10.** Materialisation of threat compromise via vulnerable devices.

### 2.3.7. Threats from Cellular Devices

Cellular devices use mobile SIM connections to provide the required functionality. These devices typically have both mobile applications and a web application. Mobile applications are typically for monitoring devices and web applications provide administrative capabilities. Smart home devices on cellular networks provide an entry point to attackers, not with a cellular connection per se, but with administration pages without authentication or weak authentication. Vulnerabilities include a lack of security processes, misconfiguration or weak configurations, and a lack of secure coding. The attack vectors are cellular devices, along with the associated applications, as they are visible on public networks/internet with a public IP address [57,61,63].

Devices with cellular networks have public IP addresses. In the absence of any integrations within the smart home environment, the impact of compromise would be restricted to the information present on the device [82]. However, any integrations of such devices with home automation within a smart environment [45] would have the same threat actors as the ones for the following threats: (a) compromise via cloud, and (b) compromise via mobile and web applications.

Threat materialisation of compromise via cellular devices using attack vectors is depicted in Figure 11.

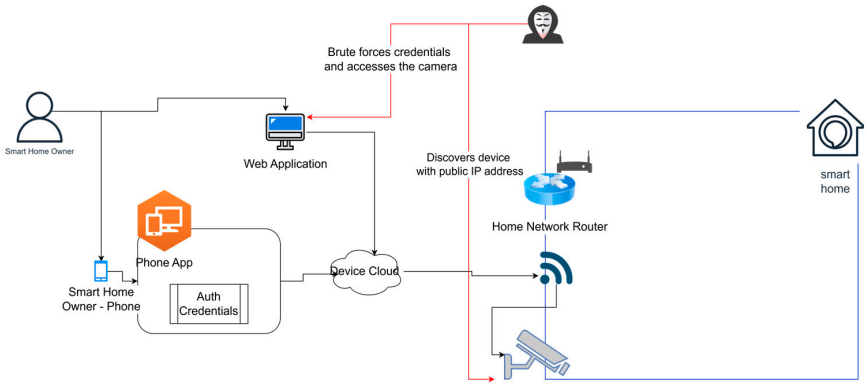


**Figure 11.** Threat materialisation of compromise via cellular devices.

### *2.4. Impact*

Compromised smart home devices have an impact on the devices and/or the smart home owner.

Threat materialisation of smart home devices that provide physical perimeter security elements, such as door locks, cameras monitoring the perimeter, and burglar alarms, could result in burglaries and bodily harm. Compromised door locks and burglar alarms could lead to malicious actors carrying out burglaries, causing bodily harm to residents in isolated locations. Compromised cameras can lead to eavesdropping, with visual and audio information leaked to threat actors, leading to an invasion of privacy [82,123,124]. Brute force attacks on SSID and Bluetooth connections result in attackers virtually entering and living in the smart home environment [46].

Cloud components of smart home devices provide functionality for remote access to the devices and to manage events from the devices. Most, if not all, smart home devices connect to a home cloud environment. The compromise of such devices could result in exfiltration of user data [125] with egress traffic. Compromised cameras can lead to eavesdropping, with visual and audio information leaked to threat actors, causing privacy compromise privacy [82,123,124] that may also result from compromise of the cloud. Any malicious traffic pushed to the smart home devices could lead to electronic eavesdropping and compromise of privacy [84].

Mobile applications and web applications provide interfaces for management and administration of smart home devices. Compromise via mobile applications and web applications may result in bodily harm, such as a boiler being disabled in winter or being set to its burning point [46]. This also includes alarms being disabled via brute force attacks on web applications.

Compromised vulnerabilities in connected devices can lead to lateral movement. This in itself is not an impact. However, (a) lateral movement to smart lights may result in the strobing of lights, causing emotional impacts [46], and (b) lateral movement to devices such as blinds or boilers may lead to unauthorised switching on or and off of devices [126], resulting in device damage.

The authors of [127] evaluated the security of smart fridges and the impact of compromise of the attack surface. Such assets have email addresses associated with owners to configure services. When email addresses are compromised and smart fridges are discovered, malicious actors may change delivery addresses, causing items to be shipped elsewhere, resulting in financial losses for the smart home owner [128].

A lack of egress traffic filtering resulted in smart fridges getting converted into bots and sending 750,000 spam emails [129]. Smart home devices can be turned into zombies/bots with second-order threats such as port forwarding. Smart fridges listening to voice commands and ordering food items lead to privacy issues with advertisements for the food items coming up on the users' social media accounts (such as Facebook) which has been documented by [130].

A lack of controls on financial information entered on integrations such as voice assistants like Alexa, Echo and Siri led to financial impacts due to unwanted purchases [131]. This is demonstrated when a child placed an order for a pricey dollhouse without the knowledge of her parents.

In line with the purchase of the pricey dollhouse enabled by a voice assistant, a different news article [132] reported deliberate and innocent prompt injections into voice assistants. As the devices keep learning prompt injections, this may result not just in financial impacts via unwanted purchases, but also privacy issues and even being a witness to crimes.

Lateral movement to devices such as laptops/desktops are second-order threats because the devices themselves do not provide any smart home device functionality, but the attacker's intention may be to get to these devices via compromise of smart home devices. The impact of second-order attacks are discussed by [133,134] when smart home devices were used in a social media attack. The opposite of this situation also works. Malware may jump on smart devices via mobile applications or administration portals.

Devices manufactured with vulnerable components lead to impacts on the physical security of the smart house. Vulnerabilities in smart devices such as smart meters (power, water) which have their own cellular connections/proprietary protocols such as z-wave can lead to malicious profiling, which in turn can lead to stalking, burglaries or bodily harm. Malicious profiling is an impact when vulnerable devices exfiltrate monitoring data to the cloud. Such devices can lead to greater compromise of smart home houses [135].

The impacts of compromised smart home devices via devices using cellular connections are not very evident at first glance, due to the challenging compromise of cellular connections (4G/5G). However, these devices are available on public networks as they have public IP addresses. As such, they are discoverable devices, as are their administration interfaces. Compromised administration interfaces or any vulnerabilities in devices can lead to breaches of privacy or a second-order attack. Examples include (a) brute forcing of default, generic credentials on the administration interface, resulting in the owner of the camera suffering a breach of privacy; (b) breach of privacy via viewing of the images; and (c) ransomware attacks by exploiting vulnerabilities in publicly available devices [82,136,137].

### *2.5. Mitigations*

Mitigations are the security [14] controls that aim to reduce the probability of threat materialisation. The other ways to treat threats and the resulting risks include (a) avoiding the threat (avoid), (b) accepting the risk of threat materialisation (accept), and (c) transferring the risk (transfer) [14].

Mitigation involves taking action to prevent a threat from materialising. Mitigating threats of physical perimeter devices via weak processes used to build smart devices

such as smart locks, are actioned by the manufacturer by adding strong processes such as authentication and authorisation or vulnerability and patching processes. However, weak authentication of near-field activation such as Bluetooth can be mitigated by the smart home owner with a verification PIN.

Some threats cannot be mitigated by a smart home owner, such as the threat of compromise via the cloud. Any weak processes such as weak vulnerability and patching process or misconfiguration of databases that expose the database to public networks/internet connections, or any missing security features such as TLS certificates can only be addressed by the manufacturer. In this scenario, the smart home owner transfers risk mitigation to the manufacturer. Similarly, the threat of compromise via vulnerable devices cannot be mitigated by the smart home owner because the owner cannot carry out assurances for the security of the firmware, the hardware, the network and any other components of the device. Here too, the owner transfers the security of devices to the manufacturers.

However, threats such as weak security processes, including weak authentication for applications, have dual responsibility. Strong authentication needs to be built into the application, which the smart home can then configure and apply. On the contrary, some materialisations of compromise via integrations can only be mitigated by the smart home owner, such as securing an MQTT server or reviewing code that is downloaded from GitHub.

### *2.6. Zero Trust in Smart Home Environments*

Compromises in smart home environments take place because resources of value exist [4]. Smart home owners access resources to either consume the offered functionality or to carry out a smart home activity. Confidentiality, integrity and availability of these assets and activities are governed by access control and authentication. With authentication, an entity proves who they are. With access control, an entity accesses the resource with the allocated permissions and privileges. Permissions are granted to an entity if there is a need for the entity to access the resource. Privileges are the granular activities that an entity can carry out with the resource.

Compromises take place if permissions and privileges are not granted correctly or if the entity is not authenticated before access is granted. This is because a malicious actor could be masquerading as the entity. A malicious actor masquerades as an authenticated entity because the environment implicitly trusts the entity, as it has provided authentication credentials at some point in time.

To reduce implicit trust, the entity needs to be authenticated before granting access to the resource. Authentication before authorisation is challenging in a smart home environment because of (a) devices manufactured with different protocols by various vendors, (b) access requests made mostly by devices than humans, and (c) nuances of device-to-device authentication and authorisation.

With such complexities and little exposure to authentication and authorisation processes of and between the devices, the following zero-trust policies can be adopted in handling the various asset categories in the environments [4].

*Need to know basis*: Need to know basis is a security construct. This construct guides people on who their information should be shared with, and more importantly, who it should not be shared with. For example, a credit card owner would not want to share the 16-digit card number, the expiry date and the CVV with anybody who asks for them. The same concept holds true in the digital world as well. Owners of the credit card should exercise caution and share the details only where required. If there is no need to share the details with a voice assistant, it should not be done.

*Least privilege*: Least privilege, as a security construct, guides people in ensuring that only the required permissions and privileges are for a device or a person to carry out activities. For example, a smart home owner should disable any unnecessary connections between assets, such as a smart fridge and a smart window blind.

*Authentication before authorisation*: This principle ensures that details of a device, its metadata or its settings are not shared without knowing who the entity is. This principle applies to devices/settings/network vectors such as SSID, near-field activation PINs. For instance, hiding SSID from external unknown actors.

*Comprehensive visibility*: This principle helps acquire information about a device and an egress connection. This principle can be used for detecting unusual occurrences in the environment. Logging everything and monitoring logs adds helps identify unusual activities with a device. This adds to situational awareness of the communication vectors and assets.

*Verified source and destination*: In an IT/OT/IoT environment, this policy would be applicable to firewall rules (which has source, destination, protocol and port), an identity allowed to access a resource, the type of device, health of device, type of API call, etc. However, in the context of a smart home environment, this policy can be applied on routers to ensure that only known and secure ports are enabled, and the endpoints of APIs are verified before enabling them on the environment. This policy is also applicable for integrations and their visibility, as any integration that has public network visibility would be visible to a malicious actor.

*Hashed credentials*: Credentials (passwords, keys, etc.) must not be stored in clear text. This is because it defeats the very purpose of having authentication. Anybody who has access to the system can go look up the credentials. However, before adding any integration, checks need to be carried out for credentials that are stored in clear text.

### *2.7. Related Work*

The past literature has focused on applying threat modelling to smart home environments. In particular, authors of [138] developed a transfer learning-based threat model for attack detection in smart homes (SALT), which is based on data flow diagrams (DFDs) and uses a transfer learning scheme to identify known and unknown threats. The authors studied threat modelling methods such as STRIDE and VAST and deduced that the methods do not identify any unknown threats in the process. Their method uses six phases which includes identifying the target environment, identifying the assets in the environment, identifying threats, generating alerts, identifying mitigations and validating the system. The method does not identify threat actors who can enter the environment via attack vectors or attack vectors [52–54] to compromise the environment.

The author [139] used DFDs and Process Flow Diagrams (PFDs) and created zones in an Internet of Things (IoT) environment, applied to a smart home use case. They threat modelled the smart home use case using STRIDE and VAST. They concluded the paper by recommending mitigations that include limiting unused services/features, implementing detection of jailbroken devices, using firewall rules for auditing and encryption of traffic. The authors do not mention anything about attack surface, entry points into smart home environment or attack paths or about supporting components such as cloud, mobile and web applications and integrations.

The authors [140,141] used STRIDE to threat model the DFDs for smart home topology. They identified threats using STRIDE threat taxonomy and applied this concept to six scenarios: (a) IP camera and IoT gateway, (b) unidirectional communication between an IP camera and the cloud, (c) bidirectional communication between an IP camera and the cloud, (d) smartphone-controlled IP camera, (e) smartphone communication with the cloud and

(f) links among smart devices. They developed network topology and simulated malware propagation in the environment. They concluded that their threat model has its limitations and threats like denial of service for physical infrastructure cannot be detected.

Security properties defined by the Federal Information Processing Standards (FIPS), such as confidentiality, integrity and availability, have been included in a threat model for smart home gateways by [142]. Along with the security properties, the researchers considered authentication, authorisation and non-repudiation. They considered assets which are (a) plugins, (b) smart home gateway application, (c) applications running on physical gateway, (d) operating system on the gateway and (e) smart home devices, with a primary focus on plugins that provide extensibility capability. Through the analysis of the use case, they deduced recommendations, including directions for developers of smart home components, which include security practices for development. The recommendations also include behaviours that should not be included in plugins. However, the authors do not consider a smart home environment as a whole and did not consider the lack of security awareness of smart home owners.

The authors of [143] have expanded STRIDE threat model method for threat analysis of smart home scenarios. They additionally used Microsoft's Security Development Lifecycle (SDL), which is used for development of software for smart home assets. They used DFDs to identify the flow of threats in the environment, identified entry points into the environment and describe assets. The authors concluded that their methods refine the approach of Microsoft's SDL and elicited various smart home scenarios with their approach. However, supporting components (cloud, applications and integrations), lack of security awareness or the disparity in the security controls of smart home devices are not considered.

Iman et al. used Arduino and Cayenne's website, along with sensors (such as sensors for motion, gas leaks, temperature changes) and an Intrusion Detection System (IDS) to identify nine possible attack scenarios for smart homes [144]. They use STRIDE to threat model the scenarios. The results of the threat model were fed into risk assessment to work out the accuracy and precision of the time delays of the sensors in smart home devices to detect anomalies in the smart home devices. The IDS improved the overall security of the smart home by providing detection services. The authors concluded that users can be alerted of the anomalies in the smart homes on the Cayenne website, which was demonstrated with their experiments. However, the authors did not consider the technical expertise, or lack of, of the smart home owners in setting up the IDS and Cayenne website.

A threat modelling method to identity privacy threats was created by Raciti et al. [145]. They named their method SPADA, which is an acronym for "Source of Documentation", "Property", "Application domain", "Detail (level of)" and "Agent(s) raising the threats". Their key research question is based on modelling (hard and soft) privacy threats. The authors define a hard threat to be a domain-independent threat and a soft threat to be domain-dependent. Their domains are a smart car and smart home environment. They combined privacy threats for smart homes to create a repository of threats. They propose that SPADA incorporates both domain-specific and non-domain-specific knowledge for threat elicitation and asset collection using the variables of "Source of Documentation", "Property", "Application domain", "Detail (level of)" and "Agent(s) raising the threats". The focus of SPADA is threat elicitation and asset collection, differing from P3CRID, which focusses on threat modelling and mitigations.

Profiling of threats caused by humans in smart home environments has been studied by [146]. The authors have identified six types of human threat actors, four motivation factors which are broad in nature and three levels of capability. The authors have used these parameters to demonstrate a scenario where a smart home has smart lighting controlled via a web application with weak authentication and authorisation. For this weakness, the

authors threat modelled the security and privacy impacts for the threats materialised via identified threat actors. The authors concluded that existing threat models have limitations and recommend security education and awareness sessions for smart home owners. The authors do not consider the mitigations that need to be added by manufacturers and the ones that need to be configured by smart home owners.

The authors of [147] threat modelled IoT-based smart home architecture. They considered threats such as (a) eavesdropping, (b) impersonation, (c) denial of service (DoS) and (d) software exploitation. They conclude that adding encryption for data in transit and using unique identifiers for access controls addresses eavesdropping and impersonation threats. However, denial of service is not addressed effectively at network layer. Similarly, software exploitation is not addressed by vendors because of lack of validation of firmware integrity and not checking for backdoors. The authors do not consider the attack vectors and the impact of the threat materialisation.

## 3. Methodology

P3CRID models threats in a smart home by first identifying assets and aligning them with applicable attack vectors. For each asset–vector pair, the methodology identifies relevant vulnerabilities, derives the corresponding threat, determines the resulting impact, and then selects mitigations. The final output is a structured threat model and a consolidated set of mitigations for the smart home environment.

Let $H$ denote a smart home environment and let

$$A = \text{identify assets } (H) = \{a_1, a_2, \ldots, a_n\}$$

be the finite set of assets. The method outputs a threat model $R$ and a mitigation set $M$, both initialised as

$$R_0 = \emptyset, \qquad M_0 = \emptyset.$$

For each asset $a \in A$, let

$$V\,(a) = \text{identify attack vectors}(a)$$

be the set of applicable attack vectors.

For each vector $v \in V\,(a)$, let

$$U(a,v) = \text{identify vulnerabilities}(a,v)$$

be the vulnerability set relevant to $(a,v)$.

For each tuple $(a,v,u)$ with $a \in A$, $v \in V\,(a)$, and $u \in U(a,v)$, define

$$t(a,v,u) := \text{identify threat}(a,v,u),$$

$$i(a,v,u) := \text{assess impact}(t(a,v,u)),$$

$$m(a,v,u) := \text{select mitigations}(a,v,u,t(a,v,u),i(a,v,u)),$$

The structured threat model record $r$, added at each iteration is:

$$r\,(a,\,v,\,u) = a,\,v,\,u,\,t(a,\,v,\,u),\,i(a,\,v,\,u),\,m(a,\,v,\,u)$$

Hence, the threat model is updated by

$$R \leftarrow R \cup \{\mathrm{r}(a,v,u)\}.$$

If mitigation is selected by the smart home owner, then the mitigation set is updated by

$$M \leftarrow M \cup m(a,v,u)$$

After all assets, attack vectors, and vulnerabilities are processed, the mitigation set is applied:

$$M \leftarrow \text{apply}(M).$$

Finally, the method returns $(R,M)$. P3CRID methodology is summarised in Algorithm 1:

**Algorithm 1:** P3CRID

Input:
Smart home environment H

Output:
Threat model R and mitigation set M

```
A ← identify_assets(H)
R ← ∅ ; M ← ∅
for each asset a ∈ A do
    V ← identify_attack_vectors(a)
    for each vector v ∈ V do
        U ← identify_vulnerabilities(a, v)
        for each vulnerability u ∈ U do
            t ← identify_threat(a, v, u)
            i ← assess_impact(t)
            m ← select_mitigations(a, v, u, t, i)
            R ← R ∪ {(a, v, u, t, i, m)}
            if mitigation_is_selected(m) then
                M ← M ∪ m
            end if
        end for
    end for
end for
M ← apply (M)
return (R, M)
```

Using P3CRID, a smart home owner starts by identifying assets/smart home devices that they own. To aid the users to identify the attack vectors, we maintain a live GitHub project (https://github.com/Shruti-s-kulkarni/smart-home-mitigations-P3CRID) that maps attack vectors to asset types and their mitigations. For readability reasons and due to the dynamic nature of threat models for smart homes, we provide examples of such Tables in the Appendix A, namely Table A1.

The owner identifies the vulnerabilities for the assets, the threats, and the impact of the threat materialisation. The owner can now look up the other files for the mitigations and the applied zero-trust principles. Based on the smart home owner's risk appetite, they can now apply the mitigations to the assets.

Zero-trust principles and their applicability to smart home environments have been discussed by the authors in [4]. These zero-trust principles were applied on the identified threats and mitigations of smart homes, based on NIST SP 800-207 and NSTAC report [4].

The following subsections demonstrate the application of P3CRID in two scenarios.

### *3.1. Applying P3CRID*

We implement P3CRID methodology using two use cases. The first use case uses an example smart home with cloud access. The second use case has an example smart home without any cloud access.

#### 3.1.1. Smart Home with Cloud Access

The architecture below is for a smart home environment that uses only Thread protocol over Wi-Fi using a bridge.

As Figure 12 depicts, the assets include (a) smart plug, (b) smart LED, (c) smart thermostat, (d) home router, and (e) the bridge. The bridge connects to the home router such that the smart plug, the smart LED and the smart thermostat can be monitored remotely. For this to take place, the devices connect to their respective clouds and to the mobile apps via Wi-Fi [148,149]. The attack vectors for this architecture include home router, mobile applications, the devices, the bridge and the clouds.

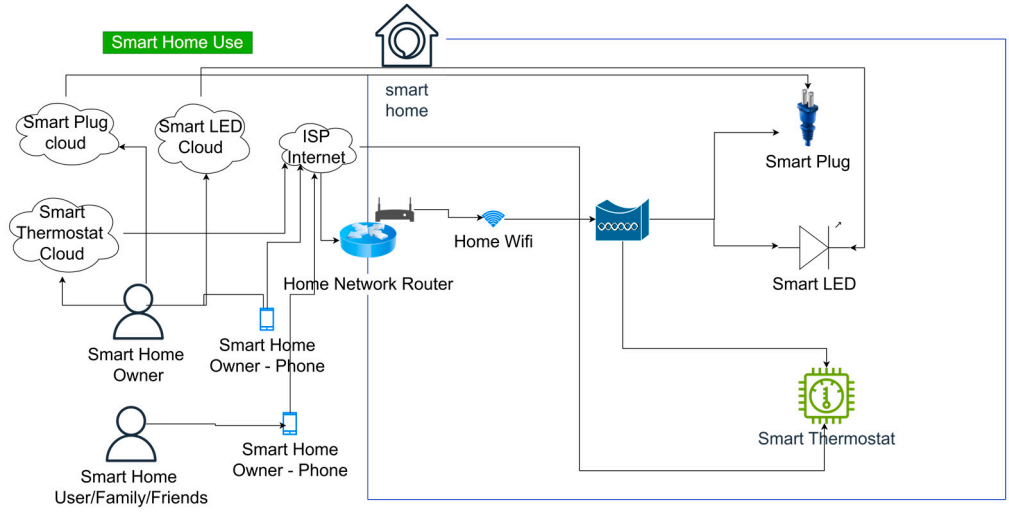


**Figure 12.** Example smart home environment with cloud-enabled devices.

The smart home environment is threat modelled using P3CRID and the results are summarised in Table 2.

**Table 2.** Threat model using P3CRID for smart home with cloud access.

| Asset Category | Assets | Threat | Attack Vectors | Vulnerabilities | Impact | Mitigations | Applied by Owners? |
|---|---|---|---|---|---|---|---|
| Near-field activated devices | Smart plug, smart LED, smart thermostat | Compromise via physical access | Physical access | Weak configurations of Bluetooth connections. | Unauthorised access to device, damage to devices, emotional impact. | Use unique verification code with Bluetooth connection. | Yes |
| | | | | Weak configurations of Bluetooth connections and SSID. | Unauthorised access to device, damage to devices, emotional impact. | Hide SSID. | Yes |
| | | | | Lack of security property of ethernet cable. | Damage to ethernet cable, resulting in lack of monitoring of devices. | Use a protective covering for the ethernet cable. | Yes |

**Table 2.** *Cont.*

| Asset Category | Assets | Threat | Attack Vectors | Vulnerabilities | Impact | Mitigations | Applied by Owners? |
|---|---|---|---|---|---|---|---|
| Cloud enabled devices | Smart Plug Cloud Smart LED Cloud Smart thermostat cloud | Compromises in cloud | Cloud | Weak configuration resulting in database being available on the internet. | Privacy compromise via unauthorised access to data, electronic eavesdropping. | Ensuring assets with sensitive data are not exposed to the internet. | No |
| | Smart Plug Cloud Smart LED Cloud Smart thermostat cloud | Compromises in cloud | Cloud | lack of security processes resulting in weak authentication for cloud administrators. | Privacy compromise, electronic eavesdropping. | Using strong authentication with MFA. | No |
| | Smart Plug Cloud Smart LED Cloud Smart thermostat cloud | Compromises in cloud | Cloud | lack of security awareness leading to phishing attack on the cloud administrators. | Privacy compromise Electronic eavesdropping | Applying effective authentication and authorisation policies along with MFA for administrators. | No |
| Application enabled devices | Smart Plug mobile/web application Smart LED mobile/web application Smart thermostat mobile/web application | Compromise via applications—mobile and web | Applications | Lack of secure coding. | Damage to the devices and to smart home via unauthorised access to security settings of the devices. | Development processes to include secure coding. | No |
| | | | | Ineffective authentication Lack of security testing | Damage to the devices and to smart home via unauthorised access to security settings of the devices. | Testing the security features of the applications. | No |
| | | | | Lack of security processes leading to unpatched devices. | Damage to the devices and to smart home. | Pushing patches to the applications regularly. | No |
| | | | | Missing security processes with weak authentication. | Damage to the devices and to smart home. | Applying MFA to web application. | Yes |
| Router connected devices | Home router | Compromise via router | Router | Misconfigurations with insecure open ports. | Unauthorised connections. | Closing insecure ports. | Yes |
| | | | | Lack of security features which allows the router to have backdoors. | Unauthorised connections. | Apply patches provided by the manufacturers. | Yes |
| Home integrated devices | Bridge | Compromise via integrations | Integrations | Lack of security features Supply chain risks | Damage to devices Emotional impact | Review security controls | Yes |
| | | | | Lack of non-repudiation. | Lack of capability to detect incidents. | Enable logging. | Yes |
| Vulnerable devices | Smart plug, smart LED, smart thermostat | Compromise via vulnerable devices | Vulnerable devices | Supply chain risks | Exfiltration of data | Review security controls of the devices. | Yes |

*Physical perimeter*: The example smart home environment does not have any smart locks or any other smart devices that secure the physical perimeter; however, the physical cable that runs from the ISP hub to the home router may get disconnected, either deliberately or accidently, which is a vulnerability. The threat materialisation would result in disconnection of internet for the smart home impacting the remote connection monitoring

of the smart home. An applicable mitigation would be to secure the cable with a protective or something similar. Any vulnerability of weak passwords for SSIDs may lead to brute force attacks. This may result in an impact with the malicious actor virtually living in the smart home. The threat may be mitigated by the smart home owner by using strong password for the SSID and also ensuring that the home router can hide the SSID [76]. The attack vector in this case is the access to the Bluetooth connections, which is an entry point into the smart home environment. The vulnerability of a malicious actor connecting to a Bluetooth connection can be mitigated by the smart home owner by ensuring that unauthorised devices are not connected with a default pairing code [150].

*Compromise via cloud*: A vulnerability with any exposed assets in the smart plug cloud, or smart LED cloud, or smart thermostat cloud would lead to unauthorised access by a malicious actor to the device data stored in the cloud. Any smart thermostat consumption data persisting in the cloud would result in an impact by allowing the malicious actor to profile the consumption data to identify time frames for burglaries or stalking. This threat cannot be addressed by the smart home owner as they do not have any control on ensuring that cloud assets are not exposed to public network/internet. The only course of action that a smart home owner can follow is to check the security rating, if available, for the smart home devices before purchase.

*Compromise via mobile applications and web applications*: Vulnerabilities such as weak credentials or vulnerabilities in the applications may provide unauthorised access to the device settings, leading to turning on and off of devices and impacting emotional aspect of the smart home owners. The unauthorised action may also end up causing damage to the devices. The threat could be mitigated by ensuring mobile applications are built with secure coding and the applications are tested. This threat cannot be addressed by the smart home owner. Like the threat of compromise via cloud, the only course of action that a smart home owner can follow is to check the security rating, if available, for the smart home devices before purchase.

*Compromise via home router*: If the Internet Service Provider (ISP) of the example smart home does not restrict access to port 7547, which is the port for ISP remote administration, the unauthorised access could lead to smart home owner being locked out of the admin panel, change SSID passwords, disable security features, install malware that may survive reboots. The mitigations would be (a) to disconnect the router from the internet, (b) factory reset it, (c) update firmware immediately, (d) change admin and SSID passwords, (e) disable remote management, (f) check all connected devices for malware, OR g) replace the router if it is old and not supported [108].

*Compromise via integrations*: Assuming the bridge is not configured to use a cellular connection and does not have a public IP address, a malicious mobile application or the malicious user who brute forced the Wi-Fi SSID may use the bridge to send malicious commands to the smart plug and/or the smart LED and/or the smart thermostat. The vulnerability of this attack chain could be mitigated by addressing the vulnerabilities in other assets such as hiding the SSID. It could also be mitigated by the owner by checking the security rating for the integration, if available before purchase.

*Compromise via vulnerable devices*: A compromised smart thermostat may send signals to the malicious users for malicious profiling, resulting in burglaries or stalking of the smart home owners. Logging and monitoring outbound connections and blocking malicious connections by the smart home owner would mitigate this risk [151]. The threat of vulnerable devices can also be mitigated by the smart home owner by checking the security rating for the smart home devices, if available before purchase.

*Compromise of devices with cellular connections*: The example smart home does not have any devices with cellular network, hence the threat is absent for the smart home. If the

assumption made for the integration is incorrect and the bridge is available on a cellular network, any vulnerabilities of the bridge would be visible on public networks/internet and discoverable. The smart home owner can mitigate this vulnerability by ensuring that the vulnerabilities on the bridge are scanned for beforehand and the findings are mitigated, or by not making the bridge available on a cellular network.

#### 3.1.2. Smart Home Without Cloud Access

Figure 13 depicts a smart home that is set up with smart devices but does not use any remote connections or remote monitoring. A Bluetooth communication vector is used without Wi-Fi [152]. It is important to note here that the devices would not be connected to the cloud.

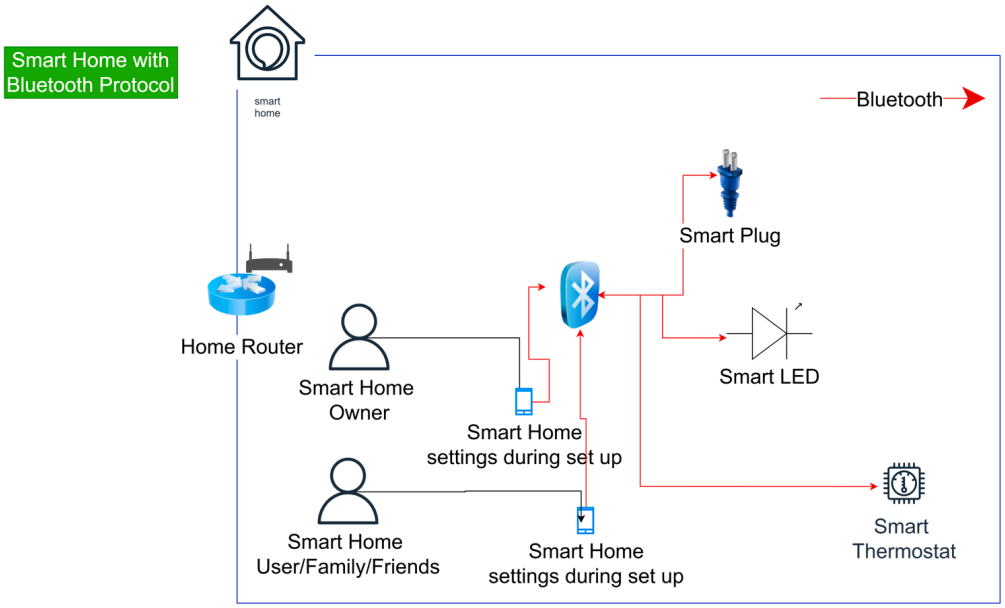


**Figure 13.** Smart home communication vectors with just Bluetooth.

The communication or the devices that run using Bluetooth are all internal to the smart home environment. The assets include (a) smart plugs, (b) smart LEDs, (c) smart thermostats, (d) home routers, and (e) mobile applications.

The smart home environment is threat modelled using P3CRID and the results are summarised in Table 3.

**Table 3.** Threat model for smart home without cloud access.

| Asset Category | Assets | Threat | Attack Vectors | Vulnerabilities | Impact | Mitigations | Applied by Owners? |
|---|---|---|---|---|---|---|---|
| Near-field activated devices | Smart plug, smart LED, smart thermostat | Compromise via physical access | Physical access | Weak configurations of Bluetooth connections. | Unauthorised access to device, Damage to devices, Emotional impact | Use unique verification code with Bluetooth connection. | Yes |
| | | | | Lack of security property of ethernet cable. | None as home router is not used by smart home devices | Use a protective covering for the ethernet cable. | Yes |

**Table 3.** *Cont.*

| Asset Category | Assets | Threat | Attack Vectors | Vulnerabilities | Impact | Mitigations | Applied by Owners? |
|---|---|---|---|---|---|---|---|
| Application enabled devices | Smart Plug mobile/web application Smart LED mobile/web application Smart thermostat mobile/web application | Compromise via applications—mobile and web | Applications | Lack of secure coding. | Damage to the devices and to smart home via unauthorised access to security settings of the devices. | Develop applications with secure coding. | No |
| | | | | Ineffective authentication. Lack of security testing. | Damage to the devices and to smart home via unauthorised access to security settings of the devices. | Testing the applications for vulnerabilities | No |
| | | | | Lack of security processes leading to unpatched devices. | Damage to the devices and to smart home. | Pushing patches to the applications regularly. | No |
| | | | | Missing security processes with weak authentication. | Damage to the devices and to smart home. | Applying MFA to web application. | Yes |
| Router connected devices | Home router | Compromise via router Compromise via vulnerable devices | Router | Misconfigurations with insecure open ports. | Unauthorised connections. | Closing insecure ports. | Yes |
| | | | | Lack of security features with backdoors. | Unauthorised connections. | Checking the security rating. | Yes |
| Vulnerable devices | Smart plug, smart LED, smart thermostat | Compromise via vulnerable devices | Vulnerable devices | Supply chain risks. | Exfiltration of data. | Review security controls of the devices. | Yes |

*Physical perimeter*: This example smart home environment does not have any smart locks or any other smart devices that secure the physical perimeter; however, the physical cable that runs from the ISP hub to the home router may get disconnected, either deliberately or accidently. The Bluetooth connections are the second threat vector that materialises the threat of physical perimeter. For a compromise to take place, the malicious actor needs to be in the vicinity of the devices, typically within 30 feet. The attack surface in this scenario may include thin walls between homes such as flats. The attack vector in this case is the access to the Bluetooth connections, which is an entry point into the smart home environment. The vulnerability of a malicious actor connecting to a Bluetooth connection can be mitigated by the smart home owner by ensuring that unauthorised devices are not connected with default pairing code [150].

*Compromise via cloud*: This threat is absent for the smart home as the devices are not connected to any cloud.

*Compromise via mobile applications and web applications*: Vulnerabilities such as weak credentials or vulnerabilities in the applications may provide unauthorised access to the device settings, leading to devices being turned on and off, causing the emotional impacts for the smart home owners. The unauthorised action may end up causing damage to the devices. The threat could be mitigated by ensuring mobile applications are built with secure coding and the applications are tested. This threat cannot be addressed by the smart home owner. Like the threat of compromise via cloud, the only course of action that a smart home owner can follow is to check the security rating for the smart home devices before purchase, if available.

*Compromise via home router*: If the Internet Service Provider (ISP) of the example smart home does not restrict access to port 7547, which is the port for ISP remote administration, the unauthorised access could lead to smart home owner being locked out of the admin

panel, change SSID passwords, disable security features, install malware that may survive reboots. The mitigations would be (a) to disconnect the router from the internet, (b) factory reset it, (c) update firmware immediately, (d) change admin and SSID passwords, (e) disable remote management, (f) check all connected devices for malware, OR (g) replace the router if it is old and not supported [108]. However, home routers are an attack vector for the example smart home only if any of the smart devices manage to connect to the SSID and exfiltrate data to a malicious cloud, because of supply chain risk. The point to be noted here is that though the device itself is not connected to the router, the router is an attack vector because of the device's ability to connect to the router being an attack vector.

*Compromise via integrations*: This threat is absent for the smart home as integrations and/or home automations are not present.

*Compromise via vulnerable devices*: Compromised devices could start scanning other Bluetooth devices and do a reconnaissance [8]. Vulnerable smart devices manage to connect to the SSID and exfiltrate data to a malicious cloud, because of supply chain risk. The point to be noted here is that though the device itself is not connected to the router, the router is an attack vector because of the device's ability to connect to the router being an attack vector.

*Compromise of devices with cellular connections*: The example smart home does not have any devices with a cellular network, hence the threat is absent for the smart home.

## 4. Evaluating P3CRID

### *4.1. Evaluation of P3CRID*

P3CRID was evaluated with the use of structured interviews (For readability reasons, the questionnaire used for the Interviews is given in the Appendix A). The study took place in the United Kingdom (UK), from November 2025 to December 2025. The study is approved by the Ethics department of the University of Hertfordshire and the UH Ethics Protocol Number is 1569 2025 Oct HSET. Participants of the evaluation of the threat model methodology—P3CRID—were recruited from communities of security professionals such as OWASP and ThreatModCon. We interviewed 12 people. The participants are cybersecurity professionals and were chosen because they are either (a) security professionals who work on threat modelling, (b) security professionals who work on threat assessments, or (c) security professionals who support threat modelling and threat assessments.

With regard to the roles of the participants, they had varying experience, i.e., Deputy Chief Technology Officer who also manages an SOC, Information Security Manager, Senior Information Security Analyst, Cloud Security Engineer, Security Architect, Application Security Architect, Senior Academic in Cybersecurity, Security Officer, Principal Security Architect, Senior Principal Security Architect, Cybersecurity Expert, Director of Security Projects.

The interviewees were taken through the P3CRID, we explained how the methodology works, requested for comments which were noted and questions regarding evaluation criteria were asked. Then, the interviewees were taken through a representative smart home environment and were requested to be hypothetically present in the smart home and to identify the threats from an owner's perspective. They were taken through a threat model developed using P3CRID to evaluate the practical application of P3CRID.

#### 4.1.1. Evaluation Criteria

For the evaluation of P3CRID, we used structured interviews using evaluation criteria proposed by NCSC [153]. The evaluation criteria cover the following requirements to validate the acquired data from the interviews and the subsequent threat models built with the methodology.

Req1: Accuracy—The accuracy criterium evaluates if the threats, assets, attack vectors, vulnerabilities, impact and mitigations applicable for smart home environment and are correct. Incorrect data or missed data elements would lead to an incomplete methodology and incomplete threat models.

Req2: Completeness—This criterium verifies the completeness of threats, assets, attack vectors, vulnerabilities, impact and mitigations to ensure that the threat materialisation, the impact and the mitigations flow together.

Req3: Uniqueness—verifies the uniqueness of the threats as any duplicated threats may dilute the methodology and result in confusion while applying the methodology.

Req4: Consistency—The criterium consolidates the threats and mitigations to ensure that the threats do not conflict with one an another and the mitigations do not conflict with one an another. Conflicts between threats and between mitigations create confusion for both threat model practitioners and for smart home owners.

Req5: Timeliness—verifies the applicability of the threats to the current prevailing threat landscape. Any misalignment would lead to (a) addressing threats that were prevalent in the past and have since been addressed in smart home devices, or (b) addressing theoretical threats of the future.

Req6: Validity—criterium verifies the required elements of a threat model methodology, such that the way a threat materialisation is identified, the impact of the threat materialisation is understood and the mitigations are identified.

#### 4.1.2. Evaluation Results

The evaluation results of P3CRID from structured interviews are summarised in Table 4.

**Table 4.** Summary of P3CRID evaluation from structured interview.

| Evaluation Criterion | Participant Feedback | Key Observations/Recommendations | Type of Feedback | Action Taken |
|---|---|---|---|---|
| Accuracy | Threats, assets, attack vectors, vulnerabilities, impacts, and mitigations in applicable to smart home environments. | No existing smart home threats were missed. | Positive | None |
| Completeness | P3CRID does not omit any threats and that its components flow logically. | Methodology is practical and easy to understand; | Positive | None |
| | | Comparative analysis with other threat models would help justify P3CRID | Area of improvement | added to the paper |
| | | More time may be required for deeper review. | Area of improvement | None |
| Uniqueness | Participants agreed that the threats identified by P3CRID are unique to the smart home environment. | Mitigations are not unique, which is expected since a single mitigation can address multiple threats. | Positive | None |
| | | Logging is missing from the list of mitigations | Area of improvement | added to the paper |
| Consistency | Most participants confirmed that threats do not conflict with one another. | Mitigations intersect while threats remain distinct; | Positive | None |
| | | Technically aware smart home owners could apply P3CRID effectively; | Positive | None |
| | | Non-technical users may find the model challenging; | Area of improvement | Added as a limitation of P3CRID to the paper |
| | | Alignment with resources such as OWASP Top 10 for IoT would improve usability. | Area of improvement | GitHub repository will capture evolving vulnerabilities. |
| Usability/ Practical Value | Helps smart home owners assess the security of their homes. | Use language accessible to both technical and non-technical users. | Area of improvement | None |
| | | Privacy breaches were confirmed as being represented in P3CRID as an impact category. | Positive | None |

**Table 4.** *Cont.*

| Evaluation Criterion | Participant Feedback | Key Observations/Recommendations | Type of Feedback | Action Taken |
|---|---|---|---|---|
| Timeliness | Threats reflect the current smart home threat landscape. | Clarification was provided that threats such as phishing and social engineering act as attack vectors. | Positive | None |
| | | Phishing leads to compromise of applications or cloud services. These vectors are included in P3CRID. | Positive | None |
| Validity | Most participants agreed that the methodology correctly identifies key threat modelling elements. | Elements include assets, attack vectors, vulnerabilities, threats, impacts, and mitigations. | Positive | None |
| | | Use open-source vulnerability databases and further examining egress information flows. | Area of improvement | GitHub repository will capture evolving vulnerabilities. |

The responses received from the evaluation of P3CRID are summarised in Table A2. For Accuracy, all participants responded with an affirmation. They all confirmed that the threats, assets, attack vectors, vulnerabilities, impact and mitigations of P3CRID are applicable for smart home environments and none of the currently existing threats for smart homes have been missed.

For Completeness, in general the participants agreed that P3CRID did not miss any threats and all the identified elements of P3CRID flowed together. Specific responses include (a) it is a good methodology and is practical for a technical person. The naming of the threats reflects the prevalent threats and is easy to understand, (b) including a comparative analysis with other threat model methodologies would help the reader understand why P3CRID should be used, which was incorporated into the paper, and (c) need more time to review P3CRID.

For Uniqueness, in general the participants agreed that P3CRID did not miss any threats and are unique for the environment. The mitigations are not unique, but that is expected as one particular mitigation may address more than one threats.

For Consistency, most participants responded by saying that threats did not conflict with one another. Specific responses include (a) the mitigations intersect but the threats are unique, which is true as evidenced in the example application of P3CRID use cases, (b) technology-aware smart home owners would be able to assess the security of their homes with P3CRID in an informed way, however technology-unaware home users may find it challenging to use the model. This is from the point of view that not enough smart home owners are engaged in threat assessments for smart homes. However, P3CRID would help a motivated smart home owner, and (c) the threat model and the mitigations need to be simplified and align to other resources for vulnerabilities, such as OWASP top 10 risks for IoT. This feedback was considered and a GitHub repository will be created to capture the dynamic nature of the vulnerabilities for smart home devices.

Most participants agreed that the methodology helps and assists the smart home owners in assessing the security of their homes. Two participants advised us to use language that would help smart home owners, with and without technical expertise. When the interviewees were asked about inclusion of privacy, all participants agreed that privacy breach was included in P3CRID as an impact.

For Timeliness, all the participants agreed that the threats are applicable to current prevailing landscape for the smart home environment. A specific question was around the inclusion of threats such as phishing. We explained that threats such as phishing and social engineering are attack vectors which lead to materialisation of threats namely (a) compromise of applications, both mobile and web, and (b) compromise via cloud. The attack vectors are included in P3CRID.

For Validity most participants agreed that the methodology identified the required fields for threat modelling which include assets, attack vectors, vulnerabilities, threats, impact and mitigations. The ingress and egress information flows did not miss any obvious ones, though edge cases may exist. Recommendations include (a) usage of open-source vulnerability databases for smart home devices to look for materialisation of attacks, especially the databases that include devices that missed patching. This feedback was considered and a GitHub repository will be created to capture the dynamic nature of the vulnerabilities for smart home devices. Another suggestion was to (b) look closely at egress flows, which was included in mitigations.

As general feedback, most participants agreed that P3CRID and the resultant threat model got the message across well. One participant asked about the type of output that would be produced. To address this, this research has developed a summarised threat model for smart home environment using P3CRID, that lists mitigations for the threats and is publicised on GitHub.

The results of the evaluation are summarised below:

(a) P3CRID is a threat model methodology that addresses the unique requirements and threats for a smart home environment, as seen from a smart home owner's perspective.

(b) P3CRID includes the current, prevalent threats for smart homes as well as captures the dynamic nature of vulnerabilities with open-source vulnerability databases.

(c) The identified threats in P3CRID methodology are unique and do not repeat when applied to smart home environments.

(d) P3CRID has practical applicability which is demonstrated in the example applications of the methodology with use cases.

## 5. Discussion and Limitations

Smart home environments are owned and operated by end users, and therefore the consequences of security compromise are experienced directly by the owners and occupants. Although smart device manufacturers implement a range of built-in security controls, a substantial portion of operational security still depends on configuration and maintenance by the owner. This challenge is compounded by the fact that smart home owners vary significantly in technical capability. As demonstrated in this paper, owners have limited ability to mitigate threats that materialise through cloud services, mobile and web applications, vulnerable device components, or cellularly connected devices, beyond performing a security review prior to purchase or deployment.

The expected users of P3CRID are (a) technology-aware smart home owners and (b) smart home device manufacturers. We also anticipate that P3CRID is useful to (a) smart home owners who are less technology-aware but use and operate interactive devices such as home automations and voice assistants, and (b) policy makers/regulatory bodies for smart home devices.

Carrying out security reviews for smart home devices is currently an activity that involves information acquisition from sources such as the manufacturer's website, open-source vulnerability disclosure databases, search engines. This puts a cognitive burden on the smart home owners to search for the required security information and the information obtained may not clearly reveal missing or inadequate security controls that are critical to secure operation. One possible way to reduce this challenge is through clear and more meaningful security markings that demonstrate the security controls of the devices. However, past research has demonstrated that smart devices that have markings that demonstrate presence of security controls can be compromised [8]. The Cyber Resilience Act (CRA) [154] has provided a mechanism for marking the devices with the designated logo by the manufacturers who have demonstrated design and implementation of security

controls. To understand the security controls implemented for the smart devices, an owner must read the specifications on the CRA manual, which adds additional burden, and may not be a relatable task for the owners. Marking the devices with security controls included in the devices and the security controls implemented during the build of the device will help an owner to make a conscious decision in the device selection process. This gap is a consideration for future work.

This situation differs somewhat for threats involving physical access, integrations, and home routers. Physical access may be compromised through weak credentials, such as insecure SSID or Bluetooth configurations, and these risks require appropriate mitigation by the owner. However, in the case of devices that provide physical security functions, such as smart locks, the owner still has limited control over the security protections built into the device and is largely restricted to assessing the device's security posture through pre-purchase or pre-deployment security review.

Home routers are used in most homes in the UK, which results in smart homes being at risk of compromises via home routers. The spring report of 2025 from Ofcom shows that at least 86% of homes in UK are connected to a home router [155]. Threats related to routers need mitigations by smart home owners, including assessing the device's security posture through pre-purchase or pre-deployment security review.

The situation is slightly different for integrations. Increased adoption of integrations as demonstrated by [156–158], are accompanied by various security and privacy threats. Based on the attack vectors and the mitigations that need applied, better control can be exercised by smart home owners over mitigations for integrations. We see two types of owners here: (a) owners implementing integrations using MQTT or using programmes from GitHub or the vendor which are implemented predominantly by those who have the necessary technical skills [159], and (b) integrations such as voice assistants that are used by both technology-aware and technology-unaware owners [159], which do not require the same level of technical skills. With increasing functionality and inter-device communication offered by integrations, better control needs exercised by smart home owners on the shared and integrated details, such as (a) credit cards details, (b) emails and calendars, (c) physical addresses, and (d) details of other smart home devices.

Because of the dynamic nature of smart home environments, the identified mitigations may require further customization as the threat landscape evolves. Emerging developments likely to influence future risk include (a) introduction of network protocol for interconnection between smart homes, (b) increasing use of cellular smart home devices, (c) guests bringing in devices with obsolete technologies such as Windows 7 or 8, (d) integration with medical devices and smart home devices [160], (e) integration with energy grids [161], and (f) smart home devices enabled for inter-device communication by default. Collectively, these developments may introduce new attack paths and dependencies, thereby necessitating periodic review of P3CRID and adaptation of mitigation strategies.

As we have discussed in Section 4, P3CRID was evaluated with the use of structured interviews with cybersecurity industry experts. While the evaluation is expert-based, primarily qualitative and not generalizable, the evaluation results of P3CRID highlighted an important practical concern, namely that many smart home owners are not actively engaged in assessing the threats affecting their environments. To address differences in user perspectives, limited technical capability, and the overlap between technology-aware and technology-unaware usage scenarios, we incorporated zero-trust policies into the mitigations for the following threats, (a) compromise via physical access, (b) compromise via home router, (c) compromise via integrations, and d) compromise via mobile and web applications, which are made available on GitHub (https://github.com/Shruti-s-kulkarni/smart-home-mitigations-P3CRID).

The authors of [4] have discussed and elaborated on how zero-trust five-step process can be applied for smart home environments. Building on that work, this paper addresses one of the gaps they identified by developing zero-trust policies to support the application of preventive controls by the smart home owners. The aim is to provide guidance to smart home owners on using preventive controls to address the threats for the functionality of the smart home devices the owners choose to use.

As highlighted by one of the interviewees, the language of P3CRID and the resulting mitigations are better understood by smart home owners who have the necessary technical expertise, but not so much who lack expertise. The gap for future research project consideration is identification of a forum to publicise the zero-trust policies and mitigations to support technology-unaware users to help understand the threats and why security matters. Education and awareness for smart home owners are discussed by [46,50]. As a part of this paper, we have created a GitHub (https://github.com/Shruti-s-kulkarni/smart-home-mitigations-P3CRID) repository to publicise zero-trust policies and the mitigations. Publicising this repository can be taken forward by authorities [162], universities and by organisations that are influential in the smart home environment space.

## 6. Conclusions

Securing smart home environments with multiple categories of assets is not a straightforward activity. It is a complex one involving security controls offered and built by the manufacturers into the smart home devices, the smart home owners' approach towards security of the devices and the resulting settings that are configured on the devices, integrations and the accompanying applications.

With complexities and varying technical skillsets of the owners, industry needs to reduce the cognitive burden on the owners such that owners can operate smart homes without having to concern themselves about threats such as malicious purchases via prompt injections, exfiltration of data via malicious smart device or a missed security control on an MQTT server. To address these situations, the smart home owner needs to understand threats applicable to their smart homes. The threat modelling methodology P3CRID, introduced in this paper, specifically targets smart home environments. The methodology is a structured, domain-specific one for this environment that can be applied by smart home owners to identify the assets that they have and the threats that are applicable to them. P3CRID assists a smart home owner in identifying the devices in the environment and in identifying the applicable mitigations for their devices.

However, P3CRID needs to be shared with smart home owners, not just for the currently available mitigations but also to understand the limitations of P3CRID. The sharing of using zero-trust policies aims to support addressing future threat landscape, such that access to devices is controlled and is tailored to requirements that a smart home owner has. Zero-trust policies guide the owners to select settings on a smart device to address unauthorised access.

Finally, the research can be extended to make the process even more simple for the owners by (a) marking smart devices with security markings that are understood by the owners, and (b) sharing the available list of zero-trust policies and mitigations mapped to asset categories, which the owners can access and apply to address the threats applicable to them.

**Author Contributions:** Conceptualization, S.K.; methodology, S.K.; validation, S.K., A.M. and S.V.; formal analysis, S.K.; investigation, S.K.; data curation, S.K. and A.M.; writing—original draft preparation, S.K.; writing—review and editing, S.K. and A.M.; visualisation, S.K.; supervision, A.M. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Supporting results can be found on GitHub at https://github.com/Shruti-s-kulkarni/smart-home-mitigations-P3CRID.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Appendix A

Questionnaire used with the interviews

- What is your job title?
- Does the threat model methodology include the threats that are applicable to a smart home environment?
- Are the threats proposed by the methodology, unique?
- Do the mitigations for the threats conflict with one another?
- Are the threats applicable to the current prevailing threat landscape for smart home environment?
- Does the method include the required elements for a threat model methodology including but not limited to threats, vulnerabilities and mitigations?
- Does the methodology capture the smart home environment in completeness including but not limited to devices or device categories, ingress and egress information flows, threat boundaries?
- Does the methodology enable a smart home owner to assess security of their smart homes?
- Do you have any other points or feedback for the threat model methodology?

Table A1 summarises threats, mitigations, risk treatment and the implementor of the mitigations.

**Table A1.** A snapshot summary of treatment of threats and risks.

| Threats | Mitigations | Risk Treatment | Design and Implementation of Mitigations | Configuration of Mitigations |
|---|---|---|---|---|
| P—Compromise of Physical perimeter devices | Strong authentication with near-field activations. | Mitigate | Near-field activation design and maintenance team | Smart home owner |
| | Select smart devices after reviewing security controls such as smart locks. | Mitigate | None | Smart home owner |
| | Secure ethernet cable. | Mitigate | None | Smart home owner |
| | Malicious profiling. | Transfer | Supplier/manufacturer | None |
| | Security awareness to avoid downgrade of security. | Mitigate | None | Smart home owner |
| | Security awareness to verify authenticity of service people. | Mitigate | None | Smart home owner |
| C—Compromise via cloud environment | Select smart devices that have good rating about security of the cloud component, if any. | Mitigate and transfer | Manufacturer | Smart home owner |
| C—Compromise via mobile devices and mobile applications | Strong authentication on web applications and mobile applications. | Mitigate and transfer | Manufacturer | Smart home owner |
| C—Compromise via cellular devices (only mobile data connection) | Strong authentication on web applications and mobile applications. | Mitigate and transfer | Manufacturer | Smart home owner |
| R—Compromise via home routers | Review access control rules on router. | Mitigate | None | Smart home owner |
| | Close unwanted ports on the router. | Mitigate | None | Smart home owner |
| | Monitor egress traffic. | Mitigate | None | Smart home owner |
| | Patch devices. | Mitigate and transfer | Manufacturer | Smart home owner |

**Table A1.** *Cont.*

| Threats | Mitigations | Risk Treatment | Design and Implementation of Mitigations | Configuration of Mitigations |
|---|---|---|---|---|
| I—Compromise via integrations | Using a PIN where credit card details are used. | Mitigate and transfer | Manufacturer | Smart home owner |
| | Securing devices from command injections such as on voice assistant. | Mitigate | None | Smart home owner |
| | Addressing caution before integrating smart home devices such as voice assistants with work related emails and calendars and even personal emails and calendars. | Mitigate | None | Smart home owner |
| | Reviewing code before using applications from GitHub. | Mitigate | None | Smart home owner |
| D—vulnerable devices and adapters (hardware, firmware, bridges) Supply chain compromise | Monitor egress traffic. | Mitigate | None | Smart home owner |
| | Patch devices. | Mitigate and transfer | Manufacturer | Smart home owner |
| None | Avoid using smart home devices. | Avoid | Owner | Smart home owner |
| All | Accept risk of using smart home devices. | Accept | Owner | Smart home owner |

Table A2. maps vulnerabilities to threats related to integrations which use zero-trust policy to identify the mitigation method for the threat.

**Table A2.** Attack vector: integrations.

| Vulnerabilities | Threats | Zero-Trust Policy | Mitigations to be Applied a Smart Home Owner |
|---|---|---|---|
| Lack of secure coding | Compromise via vulnerabilities in integrations downloaded from public repositories. | Authentication before authorization | Before using the code, review the code downloaded from public repositories |
| Lack of secure coding | Compromise via vulnerabilities in integrations downloaded from vendors. | Authentication before authorization | Before using the code, review the code downloaded from public repositories |
| Security misconfiguration/ weak configuration | Compromise via servers such as Mosquitto visible on public network. | Verified source and destination of the network connection | Check and confirm if any of the servers are visible on internet |
| Lack of security testing and lack of security features | Compromise via APIs that allow access to servers/home assistants over public network. | Verified source and destination of the network connection | Check documentation of the integration to confirm if any APIs allow access to servers/home assistants over public network |
| Lack of security processes | Lateral movement and compromise via lack of authentication on the integration. | Authentication before authorization | Check documentation of the integration to confirm it has authentication for users |
| Lack of security processes | Lateral movement and compromise via credentials stored in clear text. | Hashed credentials | Check documentation of the integration to confirm the credentials are not stored in clear text |
| Security misconfiguration/ weak configuration | Exfiltration of data via connection to an incorrect endpoint (for example connection to malicious slack channel in place of personal slack channel). | Verify destination endpoint | Verify the endpoint before sending data |
| Lack of security processes | Lateral movement and compromise via credentials stored in clear text and/or via lack of authentication on the integration. | Comprehensive visibility | Log and review the logs to detect unusual activities |

Table A3 maps vulnerabilities to threats related to integrations which uses zero-trust policy to identify the mitigation method for the threat.

**Table A3.** Attack vector: physical access.

| Vulnerabilities | Threats | Zero-Trust Policy | Mitigations to be Applied a Smart Home Owner |
|---|---|---|---|
| The Ethernet cable gets damaged accidently or deliberately | The ethernet cable gets damaged accidently or deliberately. | Least Privilege Policy by restricting access to the cable to unauthorised people. | Secure the cable in a covering that is tamper resistant. |
| Lack of security awareness | Downgrading of security controls due to owner's lack of knowledge. | Comprehensive visibility. | (a) security markings on devices and (b) education and awareness about security controls. |
| Lack of security awareness | Malicious actors locating vulnerable people in smart home environments. | Comprehensive visibility. | Education and awareness about asking for identification before letting people in. |
| Lack of security awareness | Weak SSID credentials. | Authentication before authorization. | Set strong passwords for the SSID. |
| Lack of security awareness | Visibility of SSID. | All resource authentications and authorisations are dynamic and strictly enforced before access is allowed. | Hide SSID. |
| Lack of security awareness | Bluetooth connections. | All resource authentications and authorisations are dynamic and strictly enforced before access is allowed. | Use a verification PIN. |

## References


1. UK Parliament. Connected Technology: MPs Call on Government to Tackle Growing Problem of Tech-Enabled Domestic Abuse. 2023. Available online: https://committees.parliament.uk/committee/378/culture-media-and-sport-committee/news/196867/connected-technology-mps-call-on-government-to-tackle-growing-problem-of-techenabled-domestic-abuse/ (accessed on 3 August 2025).
2. NIST. Attack Surface Under Glossary. 2024. Available online: https://csrc.nist.gov/glossary/term/attack_surface (accessed on 3 August 2025).
3. Kulkarni, S.; Mylonas, A.; Vidalis, S. Preventing and Detecting Malware in Smart Environments. The Smart Home Case. In *Malware: Handbook of Prevention and Detection*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 395–410.
4. Kulkarni, S.; Mylonas, A.; Vidalis, S. Using the Zero Trust Five-Step Implementation Process with Smart Environments: State-of-the-Art Review and Future Directions. *Future Internet* **2025**, *17*, 313. [CrossRef]
5. Assistant, H. Integrations. 3 August 2025. Available online: https://www.home-assistant.io/integrations/?brands=featured (accessed on 30 August 2025).
6. Ye, J.; De Carnavalet, X.D.C.; Zhao, L.; Zhang, M.; Wu, L.; Zhang, W. Exposed by default: A security analysis of home router default settings. In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, Singapore, 1–5 July 2024.
7. ETSI. ETSI EN 303 645 V3.1.3 (2024-09)—CYBER;Cyber Security for Consumer Internet of Things:Baseline Requirements. September 2024. Available online: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf (accessed on 19 January 2026).
8. Allen, A.; Mylonas, A.; Vidalis, S.; Gritzalis, D. Smart homes under siege: Assessing the robustness of physical security against wireless network attacks. *Comput. Secur.* **2024**, *139*, 103687. [CrossRef]
9. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. ISO: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/27001 (accessed on 19 April 2025).
10. Alliance, C.S. Connectivity Standards Alliance Certified Products. 2025. Available online: https://csa-iot.org/csa-iot_products/ (accessed on 6 August 2025).
11. ICO. Identity Theft. Available online: https://ico.org.uk/for-the-public/identity-theft/ (accessed on 30 August 2025).
12. Blunden, M. Abusive Partners Use Home Technology to Stalk and Abuse Women, Study Shows. 2018. Available online: https://www.standard.co.uk/news/tech/abusive-partners-use-home-technology-to-stalk-and-abuse-women-study-shows-a3921386.html (accessed on 25 October 2025).
13. Phelps, K. What Does the Florida Water Supply Incident Mean for ICS Cybersecurity? 2021. Available online: https://gca.isa.org/blog/the-florida-water-supply-incident-and-ics-cybersecurity (accessed on 5 September 2025).
14. NIST. Risk Response. 2011. Available online: https://csrc.nist.gov/glossary/term/risk_response (accessed on 30 August 2025).
15. NIST. Threat Modelling. Available online: https://www.ncsc.gov.uk/collection/risk-management/threat-modelling (accessed on 30 August 2025).
16. OWASP. Threat Modeling. Available online: https://owasp.org/www-community/Threat_Modeling (accessed on 30 August 2025).

17. Shevchenko, N. Threat Modeling: 12 Available Methods. 2018. Available online: https://www.sei.cmu.edu/blog/threat-modeling-12-available-methods/ (accessed on 12 September 2025).
18. Conklin, L. Threat Modeling Process. 2025. Available online: https://owasp.org/www-community/Threat_Modeling_Process (accessed on 16 January 2026).
19. Modeler, T. VAST Threat Methodology. 2025. Available online: https://threatmodeler.com/glossary/vast-threat-methodology/ (accessed on 16 January 2026).
20. Kirtley, N. PASTA Threat Modeling. 2022. Available online: https://4598121.fs1.hubspotusercontent-na1.net/hubfs/4598121/Service-Offerings/AppSec/AppSec-Gated-Content/Versprite-PASTA-Process-for-Attack-Simultation-Threat-Analysis-ebook-2022.pdf (accessed on 16 January 2026).
21. Tidmarsh, D. Why TRIKE Is the Most Popular Threat Modeling Methodology. 2023. Available online: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/trike-threat-modeling-methodology/ (accessed on 16 January 2026).
22. Wuyts, K.; Sion, L.; Joosen, W. Linddun go: A lightweight approach to privacy threat modelling. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020.
23. Naik, N.; Jenkins, P.; Grace, P.; Naik, D.; Prajapat, S.; Song, J. A comparative analysis of threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. In *The International Conference on Computing, Communication, Cybersecurity & AI*; Springer Nature: Berlin/Heidelberg, Germany, 2024.
24. Allen-Addy, C. Threat Modeling STRIDE Methodology. Available online: https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride (accessed on 1 January 2026).
25. Hammami, A. The art of threat modelling. *J. Comput. Sci. Inform.* **2024**, *1*, 57.
26. Security.org. How Do Smart Light Bulbs Work? 2024. Available online: https://www.security.org/smart-home/smart-lights/ (accessed on 7 May 2025).
27. Currys. How to Set Up a Smart TV. 2023. Available online: https://www.currys.co.uk/techtalk/tv-advice/how-to-set-up-your-smart-tv.html (accessed on 11 May 2025).
28. Matter_Smarthome. How to Set Up a Smart Home with Matter–Step by Step. 2025. Available online: https://matter-smarthome.de/en/practice/how-to-set-up-a-smart-home-with-matter-step-by-step/ (accessed on 20 April 2025).
29. Phillips. How To Set Up Smart Bulbs and Lamps. 2025. Available online: https://www.philips-hue.com/en-gb/support/connect-hue-product/bulbs-and-lamps#bridge (accessed on 25 April 2025).
30. Samsung. User Manual. 2024. Available online: https://downloadcenter.samsung.com/content/PM/202407/20240702162336446/EN/EN-US/EN-US/RF9000_US_EN-US_c1_s1.html (accessed on 2 April 2025).
31. Tapo. How to Set Up the Tapo Camera. 2025. Available online: https://www.tp-link.com/us/support/faq/2710/ (accessed on 13 April 2025).
32. Nasir, H.; Aziz, W.B.W.; Ali, F.; Kadir, K.; Khan, S. The implementation of IoT based smart refrigerator system. In *2018 2nd International Conference on Smart Sensors and Application (ICSSA)*; IEEE: Piscataway, NJ, USA, 2018.
33. Nichols, J.; Myers, B.A. Controlling home and office appliances with smart phones. *IEEE Pervasive Comput.* **2006**, *5*, 60–67. [CrossRef]
34. Ezugwu, A.E.; Taiwo, O.; Egwuche, O.S.; Abualigah, L.; Van Der Merwe, A.; Pal, J.; Saha, A.K.; Alzahrani, A.I.; Alblehai, F.; Greeff, J.; et al. Smart Homes of the Future. *Trans. Emerg. Telecommun. Technol.* **2025**, *36*, e70041. [CrossRef]
35. Silkron. Smart Fridge Solution. Available online: https://www.silkron.com/smart-fridge#how-does-the-smart-fridge-work (accessed on 7 May 2025).
36. Matter. Matter Devices. 2025. Available online: https://www.matterdatabase.com/ (accessed on 1 August 2025).
37. Vesternet. Available online: https://www.vesternet.com/collections/ (accessed on 17 March 2026).
38. Available online: https://www.vesternet.com/collections/zigbee (accessed on 17 March 2026).
39. Available online: https://www.vesternet.com/collections/z-wave (accessed on 17 March 2026).
40. ABB. Extend your Smart Home with Integrations & Addons. 2025. Available online: https://new.abb.com/low-voltage/products/building-automation/smart-home-ecosystem (accessed on 3 January 2026).
41. Boef, H. Open-Source Tools to Connect and Control Your 'Smart Home' via MQTT and Bluetooth. 2021. Available online: https://github.com/hansb001/smarthome (accessed on 27 August 2025).
42. OpenHAB. Empowering the Smart Home. 2025. Available online: https://www.openhab.org/ (accessed on 27 August 2025).
43. SunFounder. How to Set Up a Raspberry Pi MQTT Broker: A Complete Guide. Available online: https://www.sunfounder.com/blogs/news/how-to-set-up-a-raspberry-pi-mqtt-broker-a-complete-guide?srsltid=AfmBOor8rWXaMkSlXAnAPALPjyZFklT59Usn7Hpn4YOgkkIDcxSb1Axh (accessed on 23 September 2025).
44. security.org. Is There a Security Camera That Works Without Wi-Fi? Available online: https://www.security.org/security-cameras/no-wifi/#: :text=The Arlo Go and the Reolink Go, for example, are,plans instead of Wi-Fi (accessed on 31 August 2025).
45. Wireless, C. How Can Cellular IoT Initiate Smart Homes 2.0. 2025. Available online: https://www.cavliwireless.com/blog/nerdiest-of-things/how-cellular-iot-affects-the-smart-homes-segment (accessed on 31 August 2025).

46. Heartfield, R.; Loukas, G.; Budimir, S.; Bezemskij, A.; Fontaine, J.R.J.; Filippoupolitis, A.; Roesch, E. A taxonomy of cyber-physical threats and impact in the smart home. *Comput. Secur.* **2018**, *78*, 398–428. [CrossRef]
47. Vardakis, G.; Hatzivasilis, G.; Koutsaki, E.; Papadakis, N. Review of Smart-Home Security Using the Internet of Things. *Electronics* **2024**, *13*, 3343. [CrossRef]
48. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors* **2020**, *20*, 3625. [CrossRef]
49. Sasi, T.; Lashkari, A.H.; Lu, R.; Xiong, P.; Iqbal, S. A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *J. Inf. Intell.* **2024**, *2*, 455–513. [CrossRef]
50. Alsufyani, A.; Rana, O.; Perera, C. Knowledge-based cyber physical security at smart home: A review. *ACM Comput. Surv.* **2024**, *57*, 1–36. [CrossRef]
51. NIST. Threat Under Glossary. Available online: https://csrc.nist.gov/glossary/term/threat (accessed on 30 August 2025).
52. Crowdstrike. Attack Vectors: What They Are and How They Are Exploited. 2025. Available online: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/attack-vector/ (accessed on 22 July 2025).
53. Proofpoint. Attack Vector. 2025. Available online: https://www.proofpoint.com/uk/threat-reference/attack-vector (accessed on 22 July 2025).
54. Fortinet. What Is An Attack Vector? 2025. Available online: https://www.fortinet.com/resources/cyberglossary/attack-vector#:text=An attack vector is a,breach, or steal login credentials (accessed on 22 July 2025).
55. NIST. Threat Actor Under Glossary. Available online: https://csrc.nist.gov/glossary/term/threat_actor (accessed on 30 August 2025).
56. MITRE. MITRE ATT&CK. Available online: https://attack.mitre.org/ (accessed on 4 August 2025).
57. VulDB. Vulnerability Database. 2026. Available online: https://vuldb.com/?search (accessed on 29 January 2026).
58. NIST. Vulnerability Under Glossary. Available online: https://csrc.nist.gov/glossary/term/vulnerability (accessed on 30 August 2025).
59. NIST. Weakness Under Glossary. Available online: https://csrc.nist.gov/glossary/term/weakness (accessed on 30 August 2025).
60. exploit-db. 2026. Available online: https://www.exploit-db.com/ (accessed on 29 January 2026).
61. censys. 2026. Available online: https://platform.censys.io/home (accessed on 29 January 2026).
62. NIST. Impact Under Glossary. 2018. Available online: https://csrc.nist.gov/glossary/term/impact (accessed on 30 August 2025).
63. Shodan. IP Addresses and Devices on Internet. 2025. Available online: https://www.shodan.io/dashboard (accessed on 1 August 2025).
64. Greynoise. IP Address and Devices on Internet. 2025. Available online: https://viz.greynoise.io/query/heiman (accessed on 1 August 2025).
65. Sivaraman, V.; Chan, D.; Earl, D.; Boreli, R. Smart-phones attacking smart-homes. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Darmstadt, Germany, 18–20 July 2016.
66. Bluetooth. The Bluetooth Range Estimator. 2025. Available online: https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/ (accessed on 10 December 2025).
67. Cypher, D.E.; Golmie, N.T. *NIST Priority Action Plan 2, Guidelines for Assessing Wireless Standards for Smart Grid Applications*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
68. Buil-Gil, D.; Kemp, S.; Kuenzel, S.; Coventry, L.; Zakhary, S.; Tilley, D.; Nicholson, J. The digital harms of smart home devices: A systematic literature review. *Comput. Hum. Behav.* **2023**, *145*, 107770. [CrossRef]
69. Ali, B.; Awad, A.I. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* **2018**, *18*, 817. [CrossRef]
70. Turk, K. *Locked into Stupidity: A Smart Lock Security Analysis*; William Gates Building: Cambridge, UK, 2023.
71. Docs, F. Reading NFC Cards. 2025. Available online: https://docs.flipper.net/zero/nfc/read (accessed on 18 December 2025).
72. Allen, A.; Mylonas, A.; Vidalis, S.; Gritzalis, D. Security Evaluation of Companion Android Applications in IoT: The Case of Smart Security Devices. *Sensors* **2024**, *24*, 5465. [CrossRef]
73. NCSC. Smart Devices: Using Them Safely in Your Home. 2024. Available online: https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home (accessed on 24 January 2026).
74. Vaas, L. IoT Doorbell Gave Up Wi-Fi Passwords to Anybody with a Screwdriver. 2016. Available online: https://news.sophos.com/en-us/2016/01/27/iot-doorbell-gave-up-wi-fi-passwords-to-anybody-with-a-screwdriver/ (accessed on 14 December 2025).
75. Defense, T. Stop Sharing Your Wi-Fi Password: Set Up a Guest Network Now. 2025. Available online: https://www.totaldefense.com/security-blog/stop-sharing-your-wi-fi-password-set-up-a-guest-network-now/?srsltid=AfmBOorbte8PDadLPBBMDc2-GvDxsJEZAomJ2Uf_HZLYdKq12-CHLked (accessed on 14 December 2025).
76. TP-Link. How to Hide the Network Name (SSID) of a TP-Link Router. 2020. Available online: https://www.tp-link.com/fr-be/support/faq/2653/ (accessed on 17 January 2026).

77. Forbes. Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach 2019. Available online: https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/ (accessed on 25 August 2025).
78. Zhou, W.; Jia, Y.; Yao, Y.; Zhu, L.; Guan, L.; Mao, Y.; Liu, P.; Zhang, Y. Discovering and understanding the security hazards in the interactions between {IoT} devices, mobile apps, and clouds on smart home platforms. In *28th USENIX Security Symposium (USENIX Security 19)*; USENIX: Berkeley, CA, USA, 2019.
79. Roy, R.; Sharma, N. Cloud Computing Infrastructure in Smart Home Devices. In Proceedings of the 2023 Seventh International Conference on Image Information Processing (ICIIP), Solan, India, 22–24 November 2023.
80. Hunt, M.; Randolph, K. Summary: March 9, 2021 Security Incident Report. Available online: https://www.verkada.com/uk/security-update/report/ (accessed on 11 December 2025).
81. ZDNET. Smart Home Maker Leaks Customer Data, Device Passwords. 2019. Available online: https://www.zdnet.com/article/smart-home-maker-leaks-customer-data-device-passwords/ (accessed on 25 August 2025).
82. MalwareBytes. Thousands of Private Camera Feeds Found Online. Make Sure Yours Isn't One of Them. 24 June 2025. Available online: https://www.malwarebytes.com/blog/news/2025/06/thousands-of-private-camera-feeds-found-online-make-sure-yours-isnt-one-of-them (accessed on 25 August 2025).
83. Cybersecurity. Compromise One, Control All: Smart Home Chain Attacks in Action. 2025. Available online: https://63sats.com/blog/compromise-one-control-all-smart-home-chain-attacks-in-action/ (accessed on 30 August 2025).
84. Kelion, L. Wikileaks: CIA Has Tools to Snoop via TVs. 2017. Available online: https://www.bbc.co.uk/news/technology-39193008 (accessed on 25 December 2025).
85. Ronen, E.; O'Flynn, C.; Shamir, A.; Weingarten, A.-O. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. 2017. Available online: https://eyalro.net/publication/rosw17.html (accessed on 26 August 2025).
86. Vijayan, J. Researchers Reveal How Smart Lightbulbs Can Be Hacked to Attack. 2020. Available online: https://www.darkreading.com/iot/researchers-reveal-how-smart-lightbulbs-can-be-hacked-to-attack (accessed on 28 August 2025).
87. Cross-Site Scripting Vulnerability. 2021. Available online: https://github.com/arendst/Tasmota/issues/12221 (accessed on 27 August 2025).
88. Local Access Security Issue Due to HTTP CORS Header. 2019. Available online: https://github.com/arendst/Tasmota/issues/6767 (accessed on 12 November 2025).
89. Sun, A.; Gong, W.; Shea, R.; Liu, J. A castle of glass: Leaky iot appliances in modern smart homes. *IEEE Wirel. Commun.* **2019**, *25*, 32–37. [CrossRef]
90. Das, S.R.; Chita, S.; Peterson, N.; Shirazi, B.A.; Bhadkamkar, M. Home automation and security for mobile devices. In Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Seattle, WA, USA, 21–25 March 2011.
91. Medium. XSS on Non-Traditional Platforms: Exploiting Vulnerabilities in Internet of Things (IoT) Devices. 2023. Available online: https://medium.com/@Land2Cyber/xss-on-non-traditional-platforms-exploiting-vulnerabilities-in-internet-of-things-iot-devices-fa5b809e1f53 (accessed on 1 November 2025).
92. Chui, K.T. IoT Security Breaches: Lessons Learned from XSS Incidents. 2025. Available online: https://insights2techinfo.com/iot-security-breaches-lessons-learned-from-xss-incidents/ (accessed on 5 November 2025).
93. Arghire, I. Unpatched Sceiner Smart Lock Vulnerabilities Allow Hackers to Open Doors. 2024. Available online: https://www.securityweek.com/unpatched-sceiner-smart-lock-vulnerabilities-allow-hackers-to-open-doors (accessed on 1 November 2025).
94. Ye, M.; Jiang, N.; Yang, H.; Yan, Q. Security analysis of Internet-of-Things: A case study of august smart lock. In Proceedings of the 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, GA, USA, 1–4 May 2017.
95. Garger, K. Couple Says Hackers Took over Google Nest—Then Raised Temps and Blasted Vulgar Music. 2019. Available online: https://nypost.com/2019/09/26/couple-says-hackers-took-over-google-nest-then-raised-temps-and-blasted-vulgar-music/ (accessed on 4 December 2025).
96. Maher, J. Hacker Takes Over Couple's Smart Home, Plays Vulgar Music and Raises Temperature to 90 Degrees. 23 September 2019. Available online: https://www.newsweek.com/google-nest-hack-milwaukee-1460806 (accessed on 4 December 2025).
97. Poireault, K. Thousands of ASUS Routers Hijacked in Stealthy Backdoor Campaign. 2025. Available online: https://www.infosecurity-magazine.com/news/thousands-asus-routers-compromised/ (accessed on 26 August 2025).
98. Khandelwal, S. Multiple Backdoors found in D-Link DWR-932 B LTE Router. 2016. Available online: https://thehackernews.com/2016/09/hacking-d-link-wireless-router.html (accessed on 29 August 2025).
99. Smith, M. 7,500 MikroTik Routers Compromised, Traffic Forwarded to Attackers. 2018. Available online: https://www.csoonline.com/article/566211/7500-mikrotik-routers-compromised-traffic-forwarded-to-attackers.html (accessed on 6 October 2025).
100. Maunder, M. Thousands of Hacked Home Routers Are Attacking WordPress Sites. 2017. Available online: https://www.wordfence.com/blog/2017/04/home-routers-attacking-wordpress/ (accessed on 17 December 2025).

101. Ilascu, I. Thousands of Compromised MikroTik Routers Send Traffic to Attackers. 2018. Available online: https://www.bleepingcomputer.com/news/security/thousands-of-compromised-mikrotik-routers-send-traffic-to-attackers/ (accessed on 2 November 2025).
102. scramblr. NETGEAR Devices Hidden Page List. 2025. Available online: https://github.com/scramblr/NETGEAR_ROUTER_HIDDEN_PAGES/blob/main/README.md (accessed on 2 November 2025).
103. CyberSecurity, D. TP-Link Archer C50 (EOL) Exposed: Hardcoded DES Key Allows Sensitive Config Decryption (CVE-2025-6982). 2025. Available online: https://securityonline.info/tp-link-archer-c50-eol-exposed-hardcoded-des-key-allows-sensitive-config-decryption-cve-2025-6982/ (accessed on 2 November 2025).
104. Horowitz, M. Router Attacks in the News. 2025. Available online: https://routersecurity.org/RouterNews.php (accessed on 30 October 2025).
105. Xiaomi. 2025. Available online: https://github.com/XiaoMi/ha_xiaomi_home (accessed on 27 August 2025).
106. Schoutsen, P. Disclosure: Security Vulnerabilities in Custom Integrations HACS, Dwains Dashboard, Font Awesome and Others. 2021. Available online: https://www.home-assistant.io/blog/2021/01/22/security-disclosure/ (accessed on 27 August 2025).
107. Schoutsen, P. Disclosure: Supervisor Security Vulnerability. 2023. Available online: https://www.home-assistant.io/blog/2023/03/08/supervisor-security-disclosure/ (accessed on 27 August 2025).
108. AVAST. Avast Network Inspector Alert: Device Is Accessible from the Internet. 2025. Available online: https://support.avast.com/en-gb/article/hns-wan-access/#pc. (accessed on 31 January 2026).
109. Abrishamchi, M.A.N.; Abdullah, A.H.; Cheok, A.D.; Bielawski, K.S. Side channel attacks on smart home systems: A short overview. In Proceedings of the IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 29 October–1 November 2017.
110. Acar, A.; Fereidooni, H.; Abera, T.; Sikder, A.K.; Miettinen, M.; Aksu, H.; Conti, M.; Sadeghi, A.-R.; Uluagac, S. Peek-a-boo: I see your smart home activities, even encrypted! In Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Linz, Austria, 8–10 July 2020.
111. Security, W. Millions of Apple Airplay-Enabled Devices Can Be Hacked via Wi-Fi. 2025. Available online: https://www.wired.com/story/airborne-airplay-flaws/ (accessed on 1 November 2025).
112. Bouman, A. AirPlay Flaw Exposes All Apple Devices to Hacking Over Wi-Fi—What You Need to Know. 2025. Available online: https://www.tomsguide.com/computing/malware-adware/airplay-flaw-exposes-all-apple-devices-to-hacking-over-wi-fi-what-you-need-to-know (accessed on 1 November 2025).
113. Burgess, M. Hackers Hijacked Google's Gemini AI with a Poisoned Calendar Invite to Take Over a Smart Home. 2025. Available online: https://www.wired.com/story/google-gemini-calendar-invite-hijack-smart-home/ (accessed on 2 December 2025).
114. Nassi, B.; Cohen, S.; Yair, O. Invitation Is All You Need! Promptware Attacks Against LLM-Powered Assistants in Production Are Practical and Dangerous. 2025. Available online: https://sites.google.com/view/invitation-is-all-you-need/home. (accessed on 1 November 2025).
115. Nassi, B.; Cohen, S.; Yair, O. Invitation Is All You Need: Invoking Gemini for Workspace Agents with a Simple Google Calendar Invite. 2023. Available online: https://www.safebreach.com/blog/invitation-is-all-you-need-hacking-gemini/ (accessed on 1 November 2025).
116. Rauti, S.; Laato, S.; Pitkämäki, T. Man-in-the-browser attacks against IoT devices: A study of smart homes. In *International Conference on Soft Computing and Pattern Recognition*; Springer Nature: Berlin/Heidelberg, Germany, 2020.
117. Shi, H.; He, Y.; Wang, Q.; Zhuge, J.; Li, Q.; Liu, X. Laser-based command injection attacks on voice-controlled microphone arrays. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2024**, *2024*, 654–676. [CrossRef]
118. Hammi, B.; Zeadally, S.; Nebhen, J. Security threats, countermeasures, and challenges of digital supply chains. *ACM Comput. Surv.* **2023**, *55*, 1–40. [CrossRef]
119. CEPRO. Critical Cybersecurity Vulnerabilities in Smart Home Devices Uncovered in New Research. 2024. Available online: https://www.cepro.com/news/critical-cybersecurity-vulnerabilities-in-smart-home-devices-uncovered-in-new-research/139067/ (accessed on 25 August 2025).
120. Aufranc, J.-L. Sonoff & Tuya Smart Plugs Found to Transmit Unencrypted Passwords. 2021. Available online: https://www.cnx-software.com/2021/05/20/sonoff-tuya-smart-plugs-found-to-transmit-unencrypted-passwords/ (accessed on 27 August 2025).
121. Kelly, S.M. That Security Camera and Smart Doorbell You're Using May Have Some Major Security Flaws. 2024. Available online: https://edition.cnn.com/2024/03/09/tech/smart-home-cameras-hackers-security (accessed on 11 December 2025).
122. Directorate, A.S. People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations. 2024. Available online: https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/peoples-republic-china-linked-actors-compromise-routers-and-iot-devices-botnet-operations. (accessed on 11 December 2025).
123. Clements, C. The Surveillance Invasion: IoT and Smart Devices Stealing Corporate Secrets. 2024. Available online: https://www.ciso.inc/blog-posts/the-surveillance-invasion-iot-and-smart-devices-stealing-corporate-secrets/ (accessed on 29 August 2025).

124. Kerr, D. FTC and TrendNet Settle Claim over Hacked Security Cameras. 2013. Available online: https://www.cnet.com/news/privacy/ftc-and-trendnet-settle-claim-over-hacked-security-cameras/ (accessed on 29 August 2025).
125. D'Orazio, C.J.; Choo, K.-K.R.; Yang, L.T. Data exfiltration from Internet of Things devices: IOS devices as case studies. *IEEE Internet Things J.* **2016**, *4*, 524–535. [CrossRef]
126. Udinmwen, E. Not so Smart Anymore—Researchers Hack into a Gemini-Powered Smart Home by Hijacking...Google Cal-endar? 10 August 2025. Available online: https://www.techradar.com/pro/security/not-so-smart-anymore-researchers-hack-into-a-gemini-powered-smart-home-by-hijacking-google-calendar (accessed on 26 December 2025).
127. Cardenas, M.F.; Acar, G. *Ethical Hacking of a Smart Fridge: Evaluating the Cybersecurity of an IoT Device Through Gray Box Hacking*; School of Electrical Engineering and Computer Science (EECS): Islamabad, Pakistan, 2021.
128. Neagle, C. Smart Refrigerator Hack Exposes Gmail Login Credentials. 2015. Available online: https://www.networkworld.com/article/942648/smart-refrigerator-hack-exposes-gmail-login-credentials.html (accessed on 6 January 2026).
129. NBC News. Smart Refrigerators Hacked to Send out Spam: Report. 2014. Available online: https://www.nbcnews.com/tech/internet/smart-refrigerators-hacked-send-out-spam-report-n11946 (accessed on 6 January 2026).
130. Fassler, J. Is Your Smart Fridge Spying on You? 2017. Available online: https://thecounter.org/smart-fridge-spying/ (accessed on 6 January 2026).
131. CBS News. Kindergartener Accidentally Orders Pricey Toy Through Amazon's Alexa. 2017. Available online: https://www.cbsnews.com/texas/news/kindergartener-accidentally-orders-pricey-toy-through-amazons-alexa/ (accessed on 6 January 2026).
132. Ramaswamy, C. Alexa, Sort Your Life out': When Amazon Echo Goes Rogue. 2017. Available online: https://www.theguardian.com/technology/shortcuts/2017/jan/09/alexa-amazon-echo-goes-rogue-accidental-shopping-dolls-house (accessed on 6 January 2026).
133. Flashpoint. 'Smart' Home Devices Used as Weapons in Website Attack. 2016. Available online: https://www.bbc.co.uk/news/technology-37738823 (accessed on 27 August 2015).
134. Sky News. Webcams and Thermostats Used in Sophisticated Cyber-Attack. 2016. Available online: https://news.sky.com/story/webcams-and-thermostats-used-in-sophisticated-cyber-attack-10627092 (accessed on 27 August 2025).
135. Bonaventura, D.; Esposito, S.; Bella, G. A case of smart devices that compromise home cybersecurity. *Comput. Secur.* **2025**, *151*, p104286. [CrossRef]
136. Titterington, A. Korean-Style Webcam Breach: 120,000 IP Cameras Hacked. 2025. Available online: https://www.kaspersky.co.in/blog/south-korea-120000-ip-cameras-hacked/29954/ (accessed on 10 January 2026).
137. Butler, G. Over 120,000 Home Cameras Hacked in South Korea for 'Sexploitation' Footage. 2025. Available online: https://www.bbc.com/news/articles/cj01q6p7ndlo (accessed on 10 January 2026).
138. Anand, P.; Singh, Y.; Singh, H.; Alshehri, M.D.; Tanwar, S. Salt: Transfer learning-based threat model for attack detection in smart home. *Sci. Rep.* **2022**, *12*, 12247. [CrossRef]
139. Abbas, S.G.; Zahid, S.; Hussain, F.; Shah, G.A.; Husnain, M. A threat modelling approach to analyze and mitigate botnet attacks in smart home use case. In Proceedings of the 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), Guangzhou, China, 31 December–1 January 2021.
140. Kavallieratos, G.; Chowdhury, N.; Katsikas, S.; Gkioulos, V.; Wolthusen, S. Threat analysis for smart homes. *Future Internet* **2019**, *11*, 207. [CrossRef]
141. Kavallieratos, G.; Gkioulos, V.; Katsikas, S.K. Threat analysis in dynamic environments: The case of the smart home. In Proceedings of the 2019 15th international conference on distributed computing in sensor systems (DCOSS), Santorini, Greece, 29–31 May 2019.
142. Corno, F.; Mannella, L. A threat model for extensible smart home gateways. In Proceedings of the 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech), Split/Bol, Croatia, 5–8 July 2022.
143. Beckers, K.; Faßbender, S.; Heisel, M.; Suppan, S. A threat analysis methodology for smart home scenarios. In *Proceedings of the International Workshop on Smart Grid Security*; Springer Nature: Berlin/Heidelberg, Germany, 2014.
144. Alhammadi, I.; Alblooshi, M.; Alsuwaidi, N.; Sedrani, S.; Alaryani, A.; Pavithran, D. Protecting Smart Home: Attack Scenarios, Risks & Threat Modeling. In Proceedings of the 2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 8–9 December 2022.
145. Raciti, M.; Bella, G. The SPADA methodology for threat modelling. *Int. J. Inf. Secur.* **2025**, *24*, 86. [CrossRef]
146. Bugeja, J.; Jacobsson, A.; Davidsson, P. An analysis of malicious threat agents for the smart connected home. In Proceedings of the 2017 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017.
147. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-Fovino, I.; Steri, G.; Baldini, G. Security and privacy issues for an IoT based smart home. In Proceedings of the 2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017.

148. González, G.; Humberto, J. Study of the Protocol for Home Automation Thread. Bachelor's Thesis, Universitat Politècnica de Catalunya. Universitat Politècnica de Catalunya, Barcelona, Sapin, 2017.
149. home-assistant.io. Thread Integrations. 2025. Available online: https://www.home-assistant.io/integrations/thread/ (accessed on 28 July 2025).
150. SentinalOne. Bluetooth Attacks | Don't Let Your Endpoints Down. 2025. Available online: https://www.sentinelone.com/blog/bluetooth-attacks-dont-let-your-endpoints-down/ (accessed on 17 January 2026).
151. TP-Link. Configuring Access Security. Available online: https://www.tp-link.com/us/configuration-guides/configuring_access_security/#_idTextAnchor000 (accessed on 24 January 2026).
152. Cync. Cync Light Bulbs FAQs. 2023. Available online: https://cyncsupport.gelighting.com/s/article/light-bulb-faq?language=en_US (accessed on 28 July 2025).
153. UK Government. Meet the Data Quality Dimensions, Measurements Driving Continuous Improvement. 2021. Available online: https://www.gov.uk/government/news/meet-the-data-quality-dimensions (accessed on 26 August 2025).
154. European Union. Cyber Resilience Act. 2025. Available online: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (accessed on 3 February 2026).
155. Ofcom. Connected Nations Update: Spring 2025. 2025. Available online: https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/connected-nations-update-spring-2025 (accessed on 1 February 2026).
156. Obaid, A.J. Assessment of smart home assistants as an IoT. *Int. J. Comput. Inf. Manuf. (IJCIM)* **2021**, *1*, 18–36. [CrossRef]
157. Johnson, N.; Reimer, T. The adoption and use of smart assistants in residential homes: The matching hypothesis. *Sustainability* **2023**, *15*, 9224. [CrossRef]
158. Edu, J.S.; Such, J.M.; Suarez-Tangil, G. Smart home personal assistants: A security and privacy review. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–36. [CrossRef]
159. Becks, E.; Zdankin, P.; Matkovic, V.; Weis, T. Complexity of smart home setups: A qualitative user study on smart home assistance and implications on technical requirements. *Technologies* **2023**, *11*, 9. [CrossRef]
160. Chan, M.; Estève, D.; Escriba, C.; Campo, E. A review of smart homes—Present state and future challenges. *Comput. Methods Programs Biomed.* **2008**, *91*, 55–81. [CrossRef] [PubMed]
161. El-Azab, R. Smart homes: Potentials and challenges. *Clean Energy* **2021**, *5*, 302–315. [CrossRef]
162. Ofcom. Online Safety. 2026. Available online: https://www.ofcom.org.uk/online-safety (accessed on 1 February 2026).