Journal of Information Security and Applications 91 (2025) 104054

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

CRASHED: Cyber risk assessment for smart home electronic devices

Georgios Paparis [a,*], Apostolis Zarras [a,b], Aristeidis Farao [a,c], Christos Xenakis [a,c]

[a] Department of Digital Systems, University of Piraeus, Piraeus, Greece
[b] Foundation for Research and Technology – Hellas, Heraklion, Greece
[c] InQbit Innovations SRL, Bucharest, Romania

ARTICLE INFO

Keywords:
Cyber risk assessment
Risk calculation
Smart home
MITRE ATT&CK
CAPEC

ABSTRACT

The rapid proliferation of Internet of Things (IoT) technology has enriched modern households with smart home devices, enhancing convenience, but simultaneously increasing vulnerability to cyber threats. This paper introduces *CRASHED*, an innovative cyber risk assessment methodology specifically designed for smart home ecosystems. Compared to existing approaches, *CRASHED* integrates the MITRE ATT&CK and CAPEC frameworks to systematically identify and analyze threats, vulnerabilities, and potential impacts. By employing device-specific profiling, quantitative metrics, and sophisticated weighting mechanisms, it delivers a multilayered assessment of cyber risks that accounts for asset criticality and threat severity, distinguishing it from conventional methods lacking such granularity. The novelty of *CRASHED* lies in its comprehensive evaluation of systemic vulnerabilities and domestic repercussions. Case studies on various smart home configurations demonstrate its effectiveness in modeling, analyzing, and mitigating risks compared to existing frameworks. This work represents a significant advancement in safeguarding smart home environments, underscoring the urgent need for specialized cyber risk assessment models in our interconnected era. The proposed methodology not only enhances threat detection and response, but also addresses critical gaps in vulnerability databases and risk calculation processes, offering a transformative solution to the evolving challenges of smart home cybersecurity.

1. Introduction

The rapid advancement of smart home technologies has fundamentally transformed the way individuals interact with their living spaces, ushering in a new era of convenience, efficiency, and seamless connectivity. These innovations, driven by the Internet of Things (IoT), encompass many devices: smart thermostats that optimize energy consumption, security cameras that provide real-time monitoring, smart locks that enhance home security, and voice-activated assistants that streamline daily tasks. The global smart home market is projected to reach $537.01 billion by 2030, underscoring the growing adoption of these devices [1]. What were once optional upgrades have become indispensable components of modern homes, revolutionizing daily living [2,3]. However, the widespread integration of smart devices also introduces an expanding range of cyber risks. These devices become increasingly interconnected and deeply embedded in critical household functions, creating potential entry points for cybercriminals. The vulnerabilities within these systems can be exploited, leading to severe consequences such as breaches of privacy, compromised safety, and financial losses [4].

However, integrating digital technology into households has faced numerous challenges. The likelihood of cyberattacks targeting residential properties has increased with the growing prevalence of electronic gadgets in homes [5]. These attacks range from unauthorized access to personal and financial information to manipulating electronic devices in residential settings. Such activities pose significant threats to individuals' privacy and safety; these are realistic, not hypothetical, scenarios. For instance, hackers have exploited smart home networks, enabling them to control lighting systems, locks, and security cameras [6]. Another notable instance involved cyberattacks on smart homes that allowed hackers to take control of a baby monitor, using it to spy on the family and even communicate with the child through the device [7,8]. Additionally, a DDoS attack disabled the smart heating system of two housing apartments in Finland, leaving residents in the cold [9]. Furthermore, cybersecurity experts have discovered methods to gain root access to Xiaomi vacuum robots by exploiting their lidar sensors [10,11]—and so on.

Several factors significantly contribute to the vulnerabilities of smart homes to cyberattacks, creating a complex landscape of potential risks. One primary issue is that many IoT devices lack robust security

* Corresponding author.
E-mail address: gpaparis@unipi.gr (G. Paparis).

https://doi.org/10.1016/j.jisa.2025.104054

Available online 18 April 2025

measures. It is worth mentioning here that in this work, we use the terms IoT devices and smart home devices interchangeably, as both refer to the same concept for this paper. Previous research [12] has shown that cybercriminals can easily target many of these devices due to their marginal security features. Manufacturers often prioritize cost and convenience over robust security protocols, resulting in devices that hackers can easily compromise. Common flaws, such as weak encryption standards, hardcoded passwords, and a lack of regular security updates, expose smart home devices to unauthorized access and manipulation. Beyond these technical shortcomings, user behavior plays a crucial role in smart home security [13,14]. Many users lack sufficient knowledge about the potential dangers associated with smart home technology and often underestimate the importance of cybersecurity. This lack of awareness leads to poor security practices, such as using weak or default passwords, failing to update device firmware regularly, and neglecting to configure security settings appropriately. These oversights make it easier for attackers to breach smart home networks and gain control over connected devices.

Given the increasing frequency of cyberattacks targeting smart homes [15] and the potentially severe consequences of these attacks, there is an urgent need for thorough evaluations of the threats posed by cyber vulnerabilities. As smart home adoption continues to grow, the complexity and interconnectivity of devices within these environments present entry points for hackers. Thus, identifying vulnerabilities within smart home networks is a critical first step in fortifying them against potential threats. A comprehensive analysis of the devices, communication protocols, and overall design of the smart home ecosystem is required to identify any security vulnerabilities that could be exploited by malicious actors [16]. Evaluating the potential repercussions of cyber risks is also crucial. A successful cyberattack on a smart home could result in a wide range of adverse outcomes, including unauthorized access to personal data, financial loss, and concerns about physical safety, such as tampering with security systems or remotely manipulating household appliances [17].

Safeguarding smart homes from cyber intrusions is essential due to their growing integration into contemporary life. Cyber risk assessments provide a comprehensive approach to protecting digital homes and their occupants from the potentially catastrophic consequences of cybercrime. Consequently, conducting thorough evaluations of cyber threats is imperative, emphasizing the need for ongoing research and advancement in smart home cybersecurity. Although traditional cyber risk assessment methodologies are effective for conventional IT infrastructure, they often fall short when applied to smart homes. The complexity of IoT devices, their decentralized nature, and the diverse range of protocols and standards they employ present unique challenges that require innovative risk assessment approaches [18]. Furthermore, the security risks associated with smart homes are significant; cyberattacks can lead to privacy breaches, financial losses, and even physical harm. Finally, existing methodologies lack the integration of vulnerability databases in the risk calculation process. Moreover, they fail to incorporate mechanisms for applying weighted adjustments to assess the impact of threats on assets. These significant gaps highlight the urgent need for innovative solutions that specifically address security and privacy concerns in smart homes by leveraging vulnerability databases and incorporating adjustment mechanisms to measure the impact of cyber threats precisely.

This article addresses the aforementioned gaps by presenting *CRASHED*, an innovative cyber risk assessment methodology that transcends traditional approaches, aiming to model and analyze cyber risks in smart homes.[1] *CRASHED* is designed for researchers and analysts interested in smart home systems, aiming to enhance their understanding and reasoning about the cyber threats impacting these systems. Our methodology employs the MITRE ATT&CK [19] and CAPEC [20] frameworks to effectively identify threats and vulnerabilities in smart devices within a smart home. By leveraging device profiling, *CRASHED* rigorously assesses the collective impact of identified threats from both a systemic and domestic perspective, adopting a holistic approach to the smart home environment. The calculation of threat impact is based on multiple factors and the use of quantitative metrics. The novelty of the proposed methodology lies in its ability to calculate the impact of a threat on an asset, factoring in the asset's criticality and the threat's weight. These two definitions provide both flexibility and precision in risk calculation, aligning with the unique characteristics of smart homes. To the best of our knowledge, *CRASHED* is the only methodology that integrates both MITRE ATT&CK and CAPEC.

In summary, we make the following main contributions:

- We introduce a novel cyber risk assessment methodology, *CRASHED*, which leverages the MITRE ATT&CK and CAPEC frameworks to address security and privacy issues simultaneously. The methodology grounds risk calculations in vulnerability databases and employs a weighting formula.
- We assess the efficacy of our proposed methodology in a smart home environment equipped with twelve smart devices. Additionally, we evaluate two distinct smart home scenarios, each comprising a unique subset of six devices.
- We compare *CRASHED* with existing approaches and frameworks for assessing cybersecurity risks in smart homes.

The remainder of the article is structured as follows: Section 2 provides an overview of the background, focusing on embedded devices for smart homes and the associated cybersecurity challenges. In Section 3, we present the stakeholder roles in smart home cybersecurity. Section 4 introduces *CRASHED*, our proposed cyber risk assessment methodology for smart homes. Section 5 is dedicated to the evaluation of *CRASHED*, while Section 6 addresses its limitations and suggests directions for future research. In Section 7, we compare *CRASHED* with related approaches. Finally, Section 8 concludes this article.

2. Background

This section provides an analytical overview of the MITRE ATT&CK and CAPEC frameworks, foundational elements of our proposed cyber risk methodology. We then present a catalog of commonly used smart home devices, followed by an examination of the cybersecurity challenges associated with smart home environments.

2.1. MITRE ATT&CK

The MITRE ATT&CK framework is a publicly accessible repository of information that outlines the tactics and strategies employed by cyber adversaries. Its purpose is to provide a shared vocabulary among defenders, enabling them to understand and effectively counter evolving threats. The framework details common tactics, techniques, and procedures used by attackers, facilitating the formulation of effective defensive strategies and threat models. This resource is readily accessible to various stakeholders, including the corporate sector, government entities, and the cybersecurity community, thus promoting distinct threat models and approaches. The structured format of MITRE ATT&CK enhances the significance of threat reporting by organizing behaviors beyond conventional indicators. This framework is foundational for creating targeted threat models and methodologies in various sectors, which include industry, government, and the cybersecurity product and service community.

As an extensive repository, the MITRE ATT&CK framework represents the tactics and procedures employed by cyber attackers and serves as a unifying framework for defenders to comprehend and address evolving threats, establishing a shared vocabulary. In contrast to other

[1] The source code of *CRASHED* can be found at https://github.com/UniPiSSL/CRASHED.

analogous frameworks, such as the Tactics, Techniques, and Procedures (TTPs) [21], MITRE ATT&CK delineates prevalent tactics, techniques, and procedures employed by cyber attackers, enabling the formulation of effective defensive strategies and threat models. Furthermore, the MITRE ATT&CK is accessible without charge to various entities, including the business sector, government, and the cybersecurity community. This accessibility aids in the advancement of targeted threat models and methods. Unlike other frameworks, such as the Cyber Kill Chain [22], which emphasize overarching tactics and stages of an attack, MITRE ATT&CK offers a comprehensive compilation of techniques categorized by tactics without prescribing a predetermined sequence of actions. This characteristic renders MITRE ATT&CK a more adaptable and extensively employed resource within the cybersecurity domain.

In this article, we leverage MITRE ATT&CK by utilizing various procedures to detect and analyze potential threats targeting every smart home component. Specifically, we examine each asset's classification and use it to identify threats by referencing the techniques and sub-techniques in the associated MITRE ATT&CK matrix (Section 4.2).

2.2. CAPEC

The Common Attack Pattern Enumeration and Classification (CAPEC) framework [20] is a fundamental taxonomy in cybersecurity, offering a well-organized and comprehensive collection of common attack patterns adversaries use. Each entry provides a detailed description of specific methodologies, clearly explaining threat actors' actions, tactics, and strategies. The primary objective of CAPEC is to facilitate a comprehensive understanding of cyber risks by systematically classifying attack patterns. This organized system enables identifying, classifying, and analyzing attack scenarios, significantly contributing to decision-making processes to address evolving cyber threats.

The CAPEC framework provides a structured taxonomy of known attack patterns. Each attack pattern is uniquely identified by a CAPEC ID and is accompanied by a detailed *name* and *description*. The attributes of a CAPEC attack pattern include: (*i*) Attack Prerequisites: Specifies the necessary conditions for the attack's success; (*ii*) Typical Severity: Indicates the potential impact if the attack is executed; (*iii*) Likelihood of Attack: Estimates the frequency of potential attacks; (*iv*) Execution Flow: Outlines the sequence of actions involved in the attack; (*v*) Related Weaknesses: References specific software weaknesses through Common Weakness Enumeration (CWE); (*vi*) *Resources*: Enumerates the tools, knowledge, and physical resources required for the attack; (*vii*) Mitigations: Suggests strategies and tools for preventing, detecting, and mitigating the attack; (*viii*) Example Instances: Provides real-world occurrences of the attack; (*ix*) Related Attack Patterns: Demonstrates connections to other similar patterns; (*x*) Taxonomy Mappings: References other relevant frameworks, such as the MITRE ATT&CK framework.

In this article, we utilize the taxonomy mappings attribute to establish a correlation between the identified threat on an asset and the related attack pattern of CAPEC. This mapping allows us to determine the likelihood and associated vulnerabilities of the threat, providing valuable insights into calculating the cyber risk for the asset (Section 4.5).

2.3. Embedded devices for smart homes

Smart home devices are modern advancements that boost comfort, security, and energy efficiency by using specialized hardware integrated into residential environments. These devices include embedded software designed for specific purposes. Although some categories of these devices may overlap, it is beyond the scope of this paper to classify them into rigid categories. Instead, we aim to assess their cyber risk based on their assigned category. Here is a non-exhaustive list of typical embedded devices someone may encounter in smart homes, illustrating our risk assessment approach.

Smart Lighting. These systems are advanced lighting solutions that can be controlled remotely and automatically to improve a home's ambiance, reduce energy consumption, and increase convenience. Examples include *Smart Bulbs* and *Smart Light Switches*.

Smart Thermostats. These Internet-connected devices allow remote temperature control through a web interface, voice commands, or a smartphone application. Notable examples include the *Nest Thermostat* and the *Ecobee Smart Thermostat*.

Smart Security. These systems consist of interconnected devices designed to enhance home protection. They may include *Smart Cameras*, *Smart Doorbells*, and *Smart Alarms*.

Smart Appliances. Equipped with advanced sensors, networking capabilities, and interactive control mechanisms, these appliances allow users to manage home environments and optimize energy consumption. Examples include *Smart Refrigerators*, *Smart Ovens*, and *Smart Washing Machines*.

Smart Entertainment. These devices offer high-quality media experiences through Internet connectivity and remote or voice control. Common devices in this category include *Smart TVs*, *Smart Speakers*, and *Smart Projectors*.

Smart Health. These Internet-connected tools are used to track health metrics, provide medical monitoring, and deliver tailored health insights. Examples include *Smart Scales*, *Smart Blood Pressure Monitors*, and *Smart Air Purifiers*.

Smart Pet Care. These devices assist pet owners in managing and monitoring their pets' health, activity, and safety. Examples include *Smart Feeders* and *Smart Litter Boxes*.

Smart Cleaning. These innovative gadgets automate and enhance the efficiency of cleaning processes. They can communicate with other smart home systems to provide sophisticated cleaning services, such as *Robot Vacuums* and *Robot Mops*.

Smart Water Leak and Smoke Detectors. Designed to detect and alert residents to water leaks and smoke, these devices help prevent damage and costly repairs. Examples include the *LeakSmart Water Leak Detection Kit*, *SmartThings Water Leak Sensor*, and *Google Nest Protect*.

Smart Gardening. These devices use sensors, automation, and connectivity to help homeowners maintain their gardens efficiently. They monitor soil conditions, control irrigation, and provide care recommendations, contributing to healthy plant growth. Examples include *Smart Irrigation Controllers* and *Smart Moisture Sensors*.

2.4. Cybersecurity challenges in smart homes

Despite the significant convenience offered by smart homes, characterized by their networked devices and systems, they present numerous cybersecurity challenges. These challenges stem from the complex and interconnected nature of smart home environments, where various devices and systems must work seamlessly together. As the adoption of smart home technology continues to grow, addressing these cybersecurity challenges becomes increasingly critical to ensure the safety and privacy of users. We categorize these challenges as follows.

CH1 – Device Proliferation and Interconnectivity. Smart homes, characterized by integrating numerous devices such as thermostats, cameras, door locks, lighting systems, and voice assistants, present substantial cybersecurity challenges. The interconnectivity of these devices increases the potential entry points for malicious attackers. Each device's unique security protocols and vulnerabilities further complicate the maintenance of a secure network, thereby elevating cyber risk [4, 23].

CH2 – Inconsistent and Inaccessible Cybersecurity Standards. A major obstacle is the lack of standardized cybersecurity measures applicable across various device types and manufacturers [24]. Numerous

companies produce smart home devices with varying levels of commitment to data protection, leading to weak links within the smart home ecosystem. Insufficient cybersecurity measures, such as default passwords or inadequate data encryption, can render devices vulnerable to cyberattacks, jeopardizing the entire network. Furthermore, a significant obstacle to enhancing smart home cybersecurity is the academic community's lack of free access to relevant cybersecurity standards documents [25]. Some of the most important standards are only accessible under certain restrictions, such as payment, making it challenging to access them for research projects.

CH3 – Data Privacy Concerns. Smart home devices collect substantial amounts of private and sensitive data, including daily routines, preferences, security codes, and camera footage [26]. Protecting this data from unauthorized access and maintaining its confidentiality is crucial, as data breaches or unauthorized data collection can lead to severe privacy violations [27–29]. The cybersecurity of smart homes largely depends on the users who maintain them. However, many users are unaware of best practices for securing their smart homes, often using weak passwords, failing to change default settings, and neglecting software updates.

CH4 – Integration with Legacy Systems. Smart homes frequently incorporate new devices into pre-existing network infrastructures not originally designed to meet contemporary cybersecurity standards. This integration process can inadvertently introduce security vulnerabilities. Developed before modern cybersecurity practices, legacy systems are particularly susceptible to cyberattacks when interfaced with new, potentially insecure devices. Consequently, the amalgamation of old and new technologies can create a heterogeneous network environment where outdated protocols and insufficient security measures open the system to various cyber threats, such as unauthorized access, data breaches, and malware infections [30,31]. This highlights the critical need for a comprehensive review and upgrade of cybersecurity measures to ensure smart home ecosystems' safe and secure operation.

CH5 – Physical Security Threats. Physical security, often overlooked, is equally essential in maintaining the integrity of smart home systems [32,33]. Severe cybersecurity breaches can occur if unauthorized individuals gain physical access to smart home technology. For instance, intruders can control various connected devices or disable critical security features if they access a smart home's router. This could lead to significant security risks, including unauthorized surveillance, data theft, and the disruption of essential services. Therefore, ensuring robust physical security measures, such as secure housing for network equipment and controlled access to key components, is crucial in safeguarding the overall cybersecurity of smart home environments.

CH6 – Network Security. The home network is a critical component of a smart home security system, interconnecting all smart devices within the household. Vulnerabilities within the home network, such as insecure Wi-Fi configurations or susceptible routers, can expose the entire smart home ecosystem to cyberattacks [28,34]. These vulnerabilities can be exploited to gain unauthorized access, potentially compromising the security and privacy of all connected devices. Consequently, ensuring a secure home network setup, including strong encryption, regular firmware updates, and robust passwords, is vital to protect the smart home ecosystem from potential cyber threats and attacks.

3. Different roles in smart home cybersecurity

The cyber risk assessment of a smart home involves two primary actors, each with a distinct role. The first is the cybersecurity professionals who utilize the *CRASHED* methodology to protect and fortify smart homes against cyber threats, ensuring privacy, safety, and functionality. The second is the cyber attackers who exploit vulnerabilities for malicious purposes, posing significant risks to homeowners. The following sections analyze the assumptions and constraints of these actors in the application of the *CRASHED* methodology.

3.1. Cybersecurity professionals

Cybersecurity professionals are assumed to have compiled a comprehensive and accurate inventory of all smart home devices. Precise threat identification and mitigation require access to up-to-date databases of known vulnerabilities and Common Vulnerabilities and Exposures (CVEs) specific to these devices. Standardized frameworks such as MITRE ATT&CK, CAPEC, and CWE are effective tools for identifying and analyzing threats and vulnerabilities, providing a structured approach to understanding the techniques and methods adversaries might employ against smart home devices. Furthermore, these devices are assumed to operate within typical smart home environments, adhering to common usage patterns, homeowner behaviors, and network configurations. This assumption facilitates the creation of realistic threat scenarios. The connectivity and interoperability of smart home devices, forming an integrated network that communicates through standard protocols, are also assumed, as this interconnectedness is vital for the effective management and security of the smart home ecosystem.

Within these assumptions, the scope of *CRASHED* is restricted to smart devices commonly found in residential settings, excluding specialized or commercial smart devices installed in industrial or enterprise environments. The proposed cyber risk assessment methodology also relies on publicly available data regarding vulnerabilities and attack patterns, excluding proprietary or undisclosed vulnerabilities from this evaluation. Homeowners are assumed to comply with recommended cybersecurity practices, such as regular updates and proper device configuration; however, the model accounts for non-compliance, which could introduce additional cyber risks. Finally, *CRASHED* primarily focuses on cyber threats, deliberately excluding physical security measures, as malicious actors' physical access to smart devices is considered an external factor beyond the scope of this assessment.

3.2. Adversary

It is assumed that adversaries have access to a wide range of resources and tools, including advanced hacking utilities, malware, and exploit kits, which are often obtainable via the dark web or through open-source penetration testing frameworks like Metasploit [35] and Nmap [36]. These resources enable attackers to conduct highly sophisticated and targeted cyber operations. Furthermore, these attackers possess high technical expertise, including a deep understanding of networking protocols, encryption techniques, and software vulnerabilities. Such expertise allows them to reverse-engineer firmware, bypass security mechanisms, and develop custom exploits.

Additionally, adversaries are presumed to be persistent and adaptable, capable of executing prolonged campaigns and employing advanced tactics such as spearphishing, social engineering, and leveraging zero-day vulnerabilities. They are also assumed to possess an in-depth knowledge of smart home architectures, including device interconnectivity, common communication protocols (e.g., Zigbee, Z-Wave, Wi-Fi), and typical user configurations. This knowledge assists them in identifying critical vulnerabilities and potential entry points within the smart home ecosystem.

Under these assumptions, adversaries have limited physical access to smart home devices and, therefore, rely primarily on remote exploitation techniques. They must also contend with advanced detection and response mechanisms, including intrusion detection systems (IDS), anomaly detection, and automated security updates, which can rapidly identify and neutralize malicious activities. The swift deployment of cybersecurity patches and updates by manufacturers further constrains the window of opportunity for exploiting known vulnerabilities. Finally, resource limitations, particularly regarding the time and computing power available to cyber attackers, impose constraints that render complex, resource-intensive attacks less feasible.

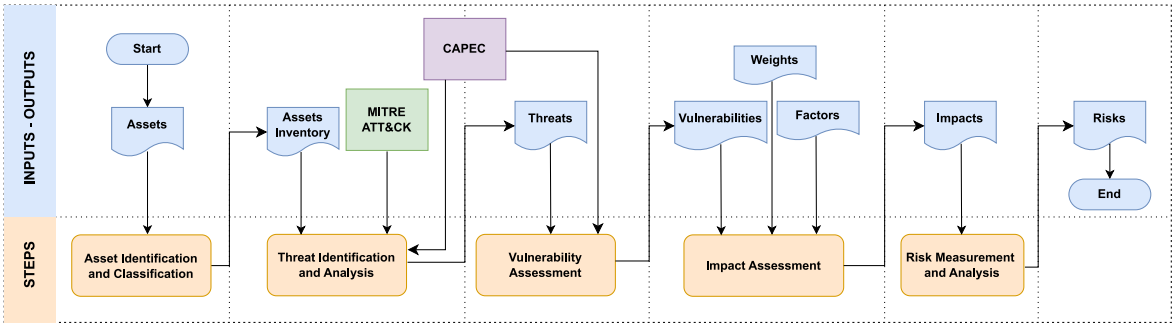

Fig. 1. *CRASHED* methodology.

3.3. A not so hypothetical scenario

Suppose an adversary gains unauthorized access to a smart home's integrated system by exploiting network vulnerabilities to orchestrate a coordinated attack. The adversary begins by disabling the smart smoke detectors, rendering them unable to detect smoke or fire. Concurrently, the adversary deactivates the smart alarm system, ensuring the homeowner remains unaware of any impending danger. With these critical safety systems compromised, the adversary remotely activates the smart oven, deliberately setting it to an extremely high temperature, potentially causing a fire. In this scenario, the smart home — once heralded as the epitome of modern convenience and security — becomes a serious safety risk under the control of a malicious entity.

While such a scenario might have seemed like science fiction just a few years ago, today it represents a genuine threat, underscoring the urgent need for a comprehensive cyber risk assessment methodology specifically tailored for smart homes [37–40]. Therefore, we propose *CRASHED* as a cyber risk assessment tool that adopts a holistic approach, considering the smart nature of devices and the potential impacts of a breach on the entire home environment.

4. Methodology

In this section, we present *CRASHED*, a cyber risk assessment methodology, which consists of five steps: (*i*) Asset Identification, (*ii*) Threat Identification and Analysis, (*iii*) Vulnerability Assessment, (*iv*) Impact Assessment, and (*v*) Risk Measurement and Analysis. Fig. 1 illustrates the steps of the proposed methodology, as well as the inputs and outputs associated with each step. *CRASHED* offers significant advantages over existing cyber risk assessment methodologies, such as OCTAVE [41].

Firstly, it provides a more granular and tailored approach to the unique environment of smart homes by categorizing assets into classes, each with distinct threat profiles and vulnerabilities. This classification facilitates a more precise threat identification and mapping process using the MITRE ATT&CK framework [19], which is more current and comprehensive compared to OCTAVE's broader, less specific threat modeling. Furthermore, the proposed methodology integrates the CAPEC [20] and CWE [42] frameworks for a detailed weakness analysis, enhancing the accuracy of vulnerability assessments.

The methodology also employs quantitative risk calculation measures, incorporating specific likelihood and impact metrics. This ensures a rigorous and systematic risk measurement process, significantly improving OCTAVE's more qualitative, subjective risk assessment approach. By leveraging real-world data from top-selling smart home devices and their known vulnerabilities, the proposed methodology provides a realistic and practical assessment that aligns closely with the dynamic nature of smart home environments. This alignment results in a more effective and actionable risk mitigation strategy.

Lastly, the *CRASHED* methodology effectively addresses the multifaceted cybersecurity challenges in smart homes (as discussed in Section 2.4). The proliferation of devices and their interconnectivity *(CH1)* are managed by toolname's systematic threat assessment across a wide range of smart devices, leveraging the MITRE ATT&CK and CAPEC frameworks to ensure that vulnerabilities unique to highly interconnected environments are thoroughly identified. *CRASHED* also addresses inconsistent cybersecurity standards *(CH2)* by applying a unified approach to threat identification and vulnerability assessment, irrespective of the manufacturer or device-specific security protocols, thereby bridging security gaps across various products. Data privacy concerns *(CH3)* are mitigated by focusing on threats that could compromise sensitive personal information, ensuring secure data flow across smart devices.

Additionally, *CRASHED* accounts for the integration of legacy systems *(CH4)*, which often lack modern cybersecurity features, by incorporating adaptive risk assessments that consider the vulnerabilities of older technologies. Physical security considerations *(CH5)* are also included, recognizing that cyber threats can emerge from physical access to smart devices. Moreover, toolname's comprehensive network security analysis ensures that weaknesses in device communications and network protocols *(CH6)* are promptly identified. This multi-layered approach enables *CRASHED* to provide a robust framework that addresses the complex and evolving cybersecurity challenges in smart home environments.

A cybersecurity risk assessment methodology for smart homes, such as the *CRASHED*, that handles sensitive user data must adhere to the following key privacy requirements to safeguard the homeowner's identity:

S1. Data Minimization: The methodology should collect and utilize only the minimal amount of information necessary to compute the overall risk. This approach reduces the likelihood of privacy violations that could expose sensitive homeowner data (e.g., CVEs associated with specific smart-home devices), potentially enabling targeted cyberattacks. Minimizing data also limits the risk that the methodology's users (e.g., cyber-insurance underwriters) may themselves become targets of cyberattacks.

S2. Data Sharing: The data employed in the cybersecurity risk assessment should not be disseminated to third parties, even those within the cybersecurity risk ecosystem, thereby preserving confidentiality and preventing unauthorized use.

S3. User Anonymity in Device Usage: The device-level cybersecurity risk analysis should be performed under conditions that approximate pseudonymity. Such measures reduce the likelihood that the homeowner can be identified through the device's associated CVEs or usage patterns.

S4. Data Origin Verification: The methodology must verify that all data utilized in the cybersecurity risk assessment is sourced from a trusted and validated environment. This ensures the methodology's integrity and protects against malfunction or misbehavior arising from spoofed or malicious inputs designed to mislead the analysis.

4.1. Asset identification and classification

The proposed cyber risk assessment methodology for smart homes begins with a critical first phase: identifying and classifying assets. This phase involves a thorough inventory of all assets within a smart home environment and then categorizing them into distinct groups based on their functions and roles. This structured approach ensures a comprehensive understanding of the components of a smart home, which is essential for effective threat detection, vulnerability assessment, and risk evaluation. The categorization process delineates three primary classes: (*i*) *Electronics & Controllers*, (*ii*) *Sensors*, and (*iii*) *Gadgets & Appliances*.

The *Electronics & Controllers* class encompasses the core components that form the backbone of a smart home network. These assets are vital for seamless integration, efficient management, and effective communication among the various smart devices. Key components in this class include network routers and gateways, such as home routers and Wi-Fi extenders, which are crucial for managing internet connectivity and enabling communication between smart devices. Smart hubs and controllers act as central units that oversee and regulate various smart home gadgets, facilitating seamless communication and automation. Additionally, smart cameras are pivotal in this category, serving as essential surveillance and security monitoring tools, providing both live and recorded video feeds. Smart doorbells with video and audio capabilities enhance security by allowing residents to monitor and communicate with visitors remotely. This class also includes smart TVs, which offer internet access and advanced features such as streaming services, voice control, and integration with home automation systems. Moreover, smart home assistants like Amazon Echo or Google Home use voice commands to control other smart devices, respond to queries, and provide information. Finally, smartphones and tablets are personal interfaces for controlling and monitoring smart home systems.

The *Sensors* class includes all devices capable of detecting and reporting on various environmental conditions. These technologies enable the automation and optimization of a smart home's environment. A key asset in this category is smart lighting, which includes intelligent lighting systems that can be remotely controlled and programmed for energy efficiency and convenience. Additionally, smart thermostats are devices that regulate heating and cooling systems, optimizing energy usage based on occupancy levels and individual user preferences. Another critical device in this category is the smart water leak sensor, which detects water leaks and potential flooding risks, thereby preventing damage. Moreover, intelligent irrigation controllers manage watering schedules for lawns and gardens, ensuring efficient water use. Finally, smart homes could use intelligent moisture sensors to monitor soil moisture levels, maintaining optimal soil conditions.

The *Gadgets & Appliances* class comprises a diverse range of smart devices designed to enhance lifestyle, convenience, and entertainment within a smart home. These devices often serve as interfaces with other smart home systems to provide a seamless user experience. Critical assets in this class include smart appliances, such as smart refrigerators, smart washing machines, and smart ovens, which offer advanced features like remote control, diagnostics, and energy management. Smart speakers and voice assistants are also important, providing households access to information, music, and home automation features through voice commands. For enhanced entertainment, smart projectors can be paired with other smart home devices to project video content. Another notable device in this class is the smart pet care system, which includes smart feeders and pet cameras that allow for the monitoring and care of pets.

By categorizing smart home assets into these classes, we establish a clear framework for analyzing the potential cyber risks associated with each type of device. This classification not only aids in identifying and understanding the unique characteristics and functions of each asset but also facilitates targeted threat identification, vulnerability assessment, and risk analysis in subsequent steps of the methodology. The outcome of the asset identification and classification phase in the proposed cyber risk assessment for smart homes is an *Assets Inventory*, which includes all smart home assets categorized into one of the aforementioned classes. This inventory serves as a foundational element for the next step.

4.2. Threat identification and analysis

The primary objective of this step is to systematically identify potential threats targeting the various smart devices within a smart home and to assess the likelihood of each threat. By utilizing the structured threat modeling frameworks of MITRE ATT&CK matrices and CAPEC, this step ensures a comprehensive and rigorous approach to threat detection.

This process begins with the *Assets Inventory* generated during the *Asset Identification and Classification* step, where each asset is classified into one of three aforementioned classes: (*i*) *Electronics & Controllers*, (*ii*) *Sensors*, and (*iii*) *Gadgets & Appliances*. Classifying assets into these classes is pivotal, as it determines the relevant MITRE ATT&CK matrix for threat identification and analysis. Each class of assets is mapped to a specific MITRE ATT&CK matrix, which provides a detailed list of adversarial techniques relevant to that category. Our model equates the techniques listed in the MITRE ATT&CK matrices to potential threats.

For assets categorized under the Electronics & Controllers class, relevant threats are derived from the *Enterprise Matrix* of MITRE ATT&CK. Notice that there may be corner cases in which the aforementioned statement does not hold. However, for the majority of the cases this statement is true. This matrix addresses threats associated with enterprise environments, which apply to devices forming the core infrastructure of a smart home network. For assets in the Sensors class, threats are mapped from the *ICS Matrix* of MITRE ATT&CK, which focuses on threats specific to industrial control environments, aligning well with the operational technologies and environmental monitoring functions of smart sensors. Finally, for assets within the Gadgets & Appliances class, the *Mobile Matrix* of MITRE ATT&CK is utilized, identifying threats related to personal gadgets and appliances that often interface with mobile technologies.

In this step, each smart device in the Assets Inventory is thoroughly analyzed against the corresponding MITRE ATT&CK matrix based on its classification. Potential threats are identified by mapping each device to the relevant adversarial techniques within the appropriate matrix. For instance, a *smart camera* from the Electronics & Controllers class is evaluated against threats from the Enterprise Matrix, identifying risks such as unauthorized access, data exfiltration, or firmware manipulation.

Next, we leverage the CAPEC database by selecting relevant attack patterns for each identified threat using the *Taxonomy Mapping* attribute. Specifically, for each threat to each asset, we select the attack patterns (CAPEC-ID) whose Taxonomy Mapping attribute includes the identified threat. In CAPEC, each attack pattern is associated with a likelihood attribute, which indicates the probability of the attack occurring, with possible values of *n/a*, *low*, *medium*, and *high*. These values are mapped to corresponding scores: 0 for n/a, 0.25 for low, 0.5 for medium, and 0.75 for high. The likelihood of each identified threat to an asset, denoted as L_{threat}, is then calculated as the median of the likelihoods from its related attack patterns. Mathematically, this is expressed as:

$$L_{\text{threat}} = \text{med}\left(L_{\text{attack pattern 1}}, \cdots, L_{\text{attack pattern n}}\right) \tag{1}$$

where L_{threat} is the likelihood of the threat to the asset, $L_{\text{attack pattern 1}}, \cdots, L_{\text{attack pattern n}}$ are the likelihoods of the related attack patterns, and n is the total number of corresponding attack patterns for the threat.

The output of the Threat Identification and Analysis step is a comprehensive list of potential threats for each smart device, along with the calculated likelihood of each threat and the corresponding attack patterns. This detailed threat profile provides a foundational understanding of each asset's cybersecurity challenges, enabling subsequent steps to focus on vulnerability assessment and risk analysis with a well-defined understanding of the threat landscape.

Table 1
Factors and subfactors of impact on systems (Heartfield et al. [43]).

Factor	Subfactor
Cyber (C)	Confidentiality (C-C) Integrity (C-I) Availability (C-A) Non-requdiation (C-NP)
Physical (P)	Breach of physical privacy (P-BPP) Unauthorized Actuation (P-UA) Incorrect Actuation (P-IA) Delayed Actuation (P-DA) Prevented Actuation (P-PA)

4.3. Vulnerability assessment

The Vulnerability Assessment step constitutes the third critical step in the cyber risk assessment methodology for smart homes. The primary goal of this phase is to identify the vulnerabilities corresponding to each threat associated with an asset. This is facilitated by leveraging the CAPEC.

Specifically, from the preceding step of Threat Identification and Analysis, it is established that each identified threat to an asset is associated with a set of attack patterns. In CAPEC, each attack pattern is linked to a set of weaknesses, which, in our model, are considered potential vulnerabilities. We define the set of vulnerabilities for each threat to an asset as the discrete union of the vulnerabilities associated with its attack patterns. Mathematically, this relationship is represented as:

$$V(T_i) = \bigcup_j V(P_{i,j}) \tag{2}$$

where T_i denotes each threat to an asset, $P_{i,j}$ represents the set of attack patterns corresponding to each threat T_i, $V(P_{i,j})$ denotes the set of vulnerabilities for each attack pattern $P_{i,j}$, and $V(T_i)$ is the set of vulnerabilities associated with each threat, defined as the union of the vulnerabilities of its attack patterns.

The output of the Vulnerability Assessment phase is a detailed profile of each threat to an asset. This profile enumerates all identified vulnerabilities related to the threat, thereby providing a comprehensive understanding of the potential security gaps that require mitigation.

4.4. Impact assessment

The Impact Assessment constitutes the fourth step of the proposed Cyber Risk Assessment Methodology. The primary objective of this step is to ascertain the potential impact of an identified threat on an asset. The impact of a threat on an asset is determined by factors. Our methodology leverages the taxonomy classification of threats proposed by Heartfield et al. [43], estimating the impacts of these threats based on two primary impact areas of factors: *Impact on Systems* and *Impact on Domestic Life*.

The Impact on Systems is divided into two factors. The first is the Cyber *(C)*, which refers to the outcomes and implications arising from occurrences or events in the digital realm. This factor is further subdivided into the following subfactors: Confidentiality *(C-C)*, Integrity *(C-I)*, Availability *(C-A)*, and Non-repudiation *(C-NP)*. The second is the (*ii*) Physical *(P)*, which pertains to the concrete effects or consequences impacting the physical environment, objects, infrastructure, or humans due to specific events, situations, or actions. This factor is subdivided into the following subfactors: Breach of Physical Privacy *(P-BPP)*, Unauthorized Actuation *(P-UA)*, Incorrect Actuation *(P-IA)*, Delayed Actuation *(P-DA)*, and Prevented Actuation *(P-PA)*. Table 1 presents the subfactors associated with each factor under *Impact on Systems*.

In turn, the Impact on Domestic Life is divided into three factors. The first is the Direct Consequences *(DC)*, which refers to the consequences that affect the financial aspects, productivity, physical health, privacy, or control of smart home devices for residents. This factor is subdivided into the following subfactors: Financial *(DC-F)*, Vocational *(DC-V)*, Invasion of Privacy *(DC-P)*, Loss of Control *(DC-LC)*, and Inconvenience *(DC-I)*. The second is the User Experience *(UX)*, which refers to the immediate or long-term impact of a threat on the user experience of the affected systems. This factor is subdivided into the following subfactors: Instantly Noticeable *(UX-N1)*, Noticeable Over Time *(UX-N2)*, and Not Noticeable *(UX-NN)*. The third is the Emotional *(E)*, which refers to consequences affecting bodily symptoms or emotional distress (e.g., the resident's perception of losing control and privacy or reduced capacity to carry out daily personal or professional activities). This factor is subdivided into the following subfactors: Appraisal *(E-A)*, Action Tendencies *(E-AT)*, Bodily Symptoms *(E-B)*, Expression *(E-E)*, and Subjective Feeling *(E-SF)*. Table 2 presents the subfactors associated with each factor under Impact on Domestic Life.

Table 2
Factors and subfactors of impact on domestic life.

Factor	Subfactor
Direct Consequences (DC)	Financial (DC-F) Vocational (DC-V) Invasion of privacy (DC-P) Loss of Control (DC-LC) Inconvenience (DC-I)
User Experience (UX)	Instantly Noticeable (UX-N1) Noticeable over time (UX-N2) Not noticeable (UX-NN)
Emotional (E)	Appraisal (E-A) Action Tendencies (E-AT) Bodily Symptoms (E-B) Expression (E-E) Subjective feeling (E-SF)

Each factor has a corresponding criticality metric for each asset. The criticality of a factor to an asset ($C_{\text{factor}_{ik}}$) measures how essential a specific factor is for the given asset. This measure is determined by considering the subfactors associated with the factor and evaluating how many of these subfactors are critical to the asset. To calculate the criticality of a factor to an asset, we use the following equation:

$$C_{\text{factor}_{ik}} = \frac{m_{\text{critical subfactors}_{ik}}}{n_{\text{total subfactors}_{ik}}} \tag{3}$$

where $C_{\text{factor}_{ik}}$ is the criticality of factor k to asset i. Similarly, $m_{\text{critical subfactors}_{ik}}$ is the number of subfactors of factor k that are critical for asset i, and $n_{\text{total subfactors}_{ik}}$ is the total number of subfactors of factor k.

The impact of a threat on an asset due to a specific factor ($I_{\text{factor}_{ijk}}$) quantifies how much a particular factor influences the overall impact of the threat on the asset. This impact is determined by considering three elements: the weight of the threat to the factor, the existence of the threat to the factor, and the criticality of the factor to the asset. To calculate the impact of a threat on an asset due to a factor, we use the following equation:

$$I_{\text{factor}_{ijk}} = W_{\text{factor}_{ijk}} \times E_{\text{factor}_{ijk}} \times C_{\text{factor}_{ik}} \tag{4}$$

where $I_{\text{factor}_{ijk}}$ is the impact of threat j on asset i due to factor k, $W_{\text{factor}_{ijk}}$ is the weight of threat j to factor k for asset i (representing the relative importance or severity of the threat concerning the factor, with values ranging from 0 to 1), $E_{\text{factor}_{ijk}}$ is the existence of threat j to factor k for asset i (indicating whether the threat is present or applicable to the factor, with values of 0 or 1), and $C_{\text{factor}_{ik}}$ is the criticality of factor k to asset i (quantifying how essential the factor is to the asset, based on the ratio of critical subfactors to the total subfactors of the factor).

The impact of a threat on an asset ($I_{\text{threat}_{ij}}$) represents the total effect that a specific threat has on the asset. This impact is determined by considering the influences of all factors associated with the threat.

To calculate the impact of a threat on an asset, we use the following equation:

$$I_{\text{threat}_{ij}} = \sum_{k=1}^{P_{ij}} I_{\text{factor}_{ijk}} \tag{5}$$

where $I_{\text{threat}_{ij}}$ is the impact of threat j on asset i, P_{ij} is the number of factors influencing the impact of threat j on asset i, and $I_{\text{factor}_{ijk}}$ is the impact of threat j on asset i due to factor k. Additionally, the sum of the weights of the threat to the asset's factors ($W_{\text{factor}_{ijk}}$) represents the total contribution of all individual factors influencing the impact of a threat on an asset. This sum must equal 1, ensuring that the weights are normalized and collectively account for the entire impact of the threat. The following equation expresses this:

$$\sum_{k=1}^{P_{ij}} W_{\text{factor}_{ijk}} = 1 \tag{6}$$

where P_{ij} is the number of factors influencing the impact of threat j on asset i, and $W_{\text{factor}_{ijk}}$ is the weight of threat j to factor k for asset i.

4.5. Risk measurement and analysis

Risk measurement and analysis is the final step in our methodology. After identifying assets, along with their corresponding threats and vulnerabilities, this step is dedicated to quantitative measurement and risk analysis.

Threat to Asset Risk. The risk associated with a threat to an asset ($R_{\text{threat}_{ij}}$) quantifies the potential loss or damage that a specific threat could inflict on the asset. This risk is calculated by considering both the likelihood of the threat occurring and its impact on the asset. The risk due to a threat to an asset is determined using the following equation:

$$R_{\text{threat}_{ij}} = L_{\text{threat}_{ij}} \times I_{\text{threat}_{ij}} \tag{7}$$

where $R_{\text{threat}_{ij}}$ represents the risk posed by threat j to asset i, $L_{\text{threat}_{ij}}$ denotes the likelihood of threat j occurring for asset i — this term captures the probability or frequency of the threat occurring — and $I_{\text{threat}_{ij}}$ signifies the impact of threat j on asset i, quantifying the potential damage or loss that could result if the threat materializes.

Asset's Risk. The risk of an asset (R_{asset_i}) encapsulates the total potential loss or damage that the asset might incur due to various threats. This overall risk is determined by summing the risks posed by all individual threats to the asset. The risk of an asset is computed using the equation:

$$R_{\text{asset}_i} = \sum_{j=1}^{M_i} R_{\text{threat}_{ij}} \tag{8}$$

where R_{asset_i} is the risk of asset i, M_i is the number of threats to asset i, and $R_{\text{threat}_{ij}}$ is the risk posed to asset i by threat j.

To normalize the risk of an asset, we first calculate the maximum possible risk that the asset could face if all threats were at their highest possible impact. This maximum risk is calculated using the equation:

$$R_{\text{max asset}} = N \times R_{\text{max threat}} \tag{9}$$

where $R_{\text{max asset}}$ represents the maximum possible risk of an asset, N is the maximum number of threats, and $R_{\text{max threat}}$ is the maximum possible risk to an asset due to a threat. The risk of an asset is then normalized to a scale of 0 to 100 using the following equation:

$$R_{\text{normalized asset}_i} = \frac{R_{\text{asset}i}}{R_{\text{max asset}i}} \times 100 \tag{10}$$

where $R_{\text{normalized asset}_i}$ is the normalized risk of asset i, R_{asset_i} is the risk of asset i, and $R_{\text{max asset}_i}$ is the maximum possible risk of asset i. A normalized risk closer to 0 indicates a low risk, whereas a value closer to 100 indicates a high risk.

Smart Home Risk. The risk of a smart home ($R_{\text{SmartHome}}$) represents the total potential loss or damage that the smart home might experience due to the risks associated with its assets. This overall risk is determined by summing the normalized risks of all individual assets within the smart home. The risk of a smart home is calculated using the equation:

$$R_{\text{SmartHome}} = \sum_{i=1}^{N} R_{\text{normalized asset}_i} \tag{11}$$

where $R_{\text{SmartHome}}$ denotes the total risk of the smart home, N is the number of assets in the smart home, and $R_{\text{normalized asset}_i}$ is the normalized risk of asset i.

To normalize the risk of a smart home, we must first compute the maximum possible risk for the smart home, assuming all assets are at their highest possible risk. This is calculated using the equation:

$$R_{\text{MaxSmartHome}} = N \times R_{\text{max asset}} \tag{12}$$

where N represents the total number of assets in the smart home, and $R_{\text{max asset}}$ is the maximum possible risk of an asset within the smart home. The risk of the smart home is then normalized to a scale of 0 to 100 using the following equation:

$$R_{\text{NormalizedSmartHome}} = \frac{R_{\text{SmartHome}}}{R_{\text{MaxSmartHome}}} \times 100 \tag{13}$$

where $R_{\text{NormalizedSmartHome}}$ denotes the normalized risk of the smart home, $R_{\text{SmartHome}}$ is the risk of the smart home, and $R_{\text{MaxSmartHome}}$ is the maximum possible risk for the smart home. A normalized risk closer to 0 indicates low risk, while a value closer to 100 indicates high risk. The normalized risk of smart home can also be translated with the following qualitative form: 0 – 25 [LOW]; 26 – 50 [MEDIUM]; 51 – 75 [HIGH]; 76 – 100 [CRITICAL] (see Table 3).

Table 3
Risk level form.

Risk level	$R_{\text{NormalizedSmartHome}}$
LOW	0–25
MEDIUM	26–50
HIGH	51–75
CRITICAL	76–100

Additionally, an algorithm has been developed to facilitate the risk calculation for each asset, as detailed in Algorithm 1. This algorithm systematically computes the risk associated with each asset within a defined set (*Line 1*), iterating through each asset to identify potential threats (*Lines 2–10*). Initially, each asset is classified (*Line 3*), followed by identifying associated threats (*Line 4*). Subsequently, the likelihood of each identified threat is calculated using the CAPEC methodology (*Line 6*). Concurrently, the impact of each threat is assessed (*Line 7*). The overall risk for each threat is then computed by multiplying the likelihood and impact scores (*Line 8*).

Algorithm 1 *CRASHED*'s risk calculation

```
1:  procedure RiskCalculate(assets, CAPEC)
2:      for each asset in assets do
3:          asset ← Classify(asset)
4:          threats_of_asset ← IdentifyThreats(asset)
5:          for each threat in threats_of_asset do
6:              Likelihood ← CalculateLikelihood(threat, CAPEC)
7:              Impact ← CalculateImpact(threat)
8:              Risk ← Likelihood × Impact
9:          end for
10:     end for
11: end procedure
```

In a nutshell, the proposed methodology is intended to guide cybersecurity professionals through its defined steps and leverage its outcomes to determine whether a smart home is sufficiently exposed to a given risk. If the aggregated risk assessment result falls into the high or critical risk category, the expert can decompose it by each

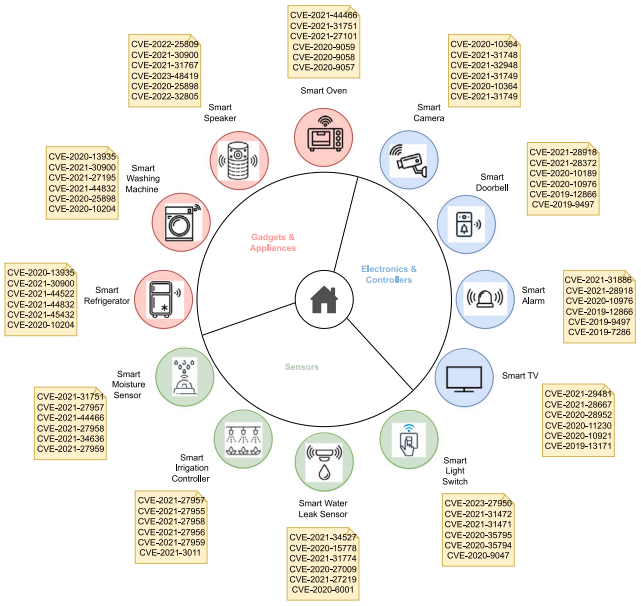

Fig. 2. Smart home and indicative CVEs.

asset, review the individual risks, and prioritize mitigation efforts accordingly. Essentially, the cybersecurity professional employs the *Risk Measurement* step to determine the normalized risk of the smart home and classify the total risk level as critical, high, medium, or low. In cases where the overall risk is identified as critical or high, the professional returns to the normalized risk values of individual assets and mitigates the highest risks first, thereby reducing the overall risk of the system.

5. Evaluation

In this section, we apply our proposed cyber risk assessment methodology to a case study involving a smart home equipped with commonly-used smart devices. The primary objective is to evaluate the risks posed by cyber threats in a smart home environment, with the ultimate goal of supporting efforts to manage these risks.

5.1. Asset identification and classification

A typical smart home setup was considered for the evaluation, comprising devices from three primary categories: (*i*) *Electronics & Controllers*, (*ii*) *Sensors*, and (*iii*) *Gadgets & Appliances*. The Electronics & Controllers category includes smart cameras, smart doorbells, smart alarms, and smart TVs. The Sensors category includes smart light switches, smart water leak sensors, smart irrigation controllers, and smart moisture sensors. The Gadgets & Appliances category includes smart refrigerators, smart washing machines, smart speakers, and smart ovens. To ensure a realistic evaluation scenario, top-selling brands of smart devices were chosen within each category. These devices inherit the vulnerabilities and CVEs associated with their respective brands and models, offering a comprehensive basis for assessing the cyber risks inherent in modern smart home environments, as illustrated in Fig. 2.

The Assets Inventory serves as the foundation for the subsequent steps of *CRASHED*. Using this inventory, we can identify the threats and vulnerabilities associated with each asset and ultimately determine the total risk for the smart home. As mentioned in Section 4, the total risk is calculated as the normalized sum of the individual risks for each asset listed in the Assets Inventory.

Inside View: It is worth to be mentioned here that given the space constraints and the primary focus of this article on demonstrating our methodology rather than exhaustively listing all vulnerabilities for every device, we will narrow our focus to a single device (i.e., a smart camera) for the purpose of illustrating our examples. However, it is important to note that the risk assessment calculations will still encompass all devices within the smart home setup. This approach allows us to effectively showcase the application of our methodology without overwhelming the reader with extensive details on each individual device.

Table 4
Top-5 threats of the selected smart camera.

Threat	CAPEC-IDs	Likelihood
Dynamic Linker Hijacking	13, 640	0.50
Impair Command History Logging	13	0.75
Brute Force	49	0.50
Process Discovery	573	0.25
Rootkit	552	0.50

Table 5
CWEs of the selected smart camera.

Threat	CWEs
Dynamic Linker Hikacking	15, 20, 73, 74, 114, 200, 285, 302, 353, 829
Impair Command History Logging	15, 20, 73, 74, 200, 285, 302, 353
Brute Force	262, 263, 257, 654, 307, 308, 309, 521
Process Discovery	200
Rootkit	284

5.2. Threat identification and analysis

After identifying and classifying the assets of the smart home and recording them in the Assets Inventory, the next step is to identify the threats associated with each asset and calculate the likelihood of these threats. Following the methodology outlined in Section 4.2, we first identify the threats based on the classification of each asset. For assets classified under Electronics & Controllers all threats from the Enterprise Matrix of MITRE ATT&CK are inherited. Similarly, assets classified under Sensors inherit all threats from the ICS Matrix of MITRE ATT&CK. In the same way, assets classified under Gadgets & Appliances inherit all threats from the Mobile Matrix of MITRE ATT&CK. Next, for each identified threat associated with the assets, we select the relevant attack patterns (CAPEC-ID) whose Taxonomy Mappings attribute contains the identified threat. Finally, the likelihood of each identified threat is calculated according to the methodology described in Section 4.2.

To provide an inside view, we utilize a specific device: a smart camera associated with several distinct threats. While a similar analysis has been conducted for all individual devices, as mentioned in Section 5.1, we present only the smart camera analysis due to space constraints. By examining Table 4, we find that the *Rootkit* threat is mapped to the *Install Rootkit* attack pattern (CAPEC-ID 552) in the Taxonomy Mapping attribute, which has a likelihood of *"Medium"*, corresponding to a likelihood score of 0.5. Consequently, the likelihood of the *Rootkit* threat is determined to be 0.5. Similarly, the *Dynamic Linker Hijacking* threat is mapped to two attack patterns in the Taxonomy Mapping attribute: (*i*) the *Subverting Environment Variable Values* attack pattern (CAPEC-ID 13), which has a *"High"* likelihood (i.e., 0.75), and (*ii*) the *Inclusion of Code in Existing Process* attack pattern (CAPEC-ID 640), which has a *"Low"* likelihood (i.e., 0.25). Therefore, the likelihood of the *Dynamic Linker Hijacking* threat is calculated as 0.5, which is the median of the likelihood scores of the two aforementioned attack patterns.

5.3. Vulnerability assessment

After identifying the comprehensive set of threats to the smart home, the next step involves determining the specific vulnerabilities

Table 6
CAPEC.

CAPEC-ID	Attack pattern	Likelihood	Vulnerabilities	Taxonomy mappings
13	Subverting Environment Variable values	High	353,285, 302,74,15, 73,20,200	ENTRY ID:1562.003:ENTRY NAME:Impair Defenses:Impair Command History Logging ENTRY ID:1574.006:ENTRY NAME:Hijack Execution Flow:Dynamic Linker Hijacking ENTRY ID:1574.007:ENTRY NAME:Hijack Execution Flow:Path Interception by PATH Environment Variable
159	Redirect access to libraries	High	706	ENTRY ID:1110.001:ENTRY NAME:Brute Force:Password Guessing
552	Install Rootkit	Medium	284	ENTRY ID:1014:ENTRY NAME:Rootkit ENTRY ID:1542.003:ENTRY NAME:Pre-OS Boot:Bootkit ENTRY ID:1547.006:ENTRY NAME:Boot or Logon Autostart Execution:Kernel Modules and Extensions
573	Process Footprinting	Low	200	ENTRY ID:1057:ENTRY NAME:Process Discovery
640	Inclusion of Code in Existing Process	Low	114,829	ENTRY ID:1505.005:ENTRY NAME:Server Software Component: Terminal Services DLL ENTRY ID:1574.006:ENTRY NAME:Hijack Execution Flow: Dynamic Linker Hijacking ENTRY ID:1574.013:ENTRY NAME:Hijack Execution Flow: KernelCallbackTable ENTRY ID:1620:ENTRY NAME:Reflective Code Loading

Table 7
Factors and subfactors in assets.

		Electronics & controllers				Sensor				Gadgets & appliances			
Factor	Subfactor	Smart camera	Smart doorbell	Smart alarm	Smart TV	Smart light switch	Smart water leak sensor	Smart irrigation controller	Smart moisture sensor	Smart refrigerator	Smart washing machine	Smart speaker	Smart Oven
Cyber (C)	Confidentiality (C-C)	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗
	Integrity (C-I)	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓
	Availability (C-A)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Non-repudiation (C-NP)	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓
Physical (P)	Breach of physical privacy (P-BPP)	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
	Unauthorized Actuation (P-UA)	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓
	Incorrect Actuation (P-IA)	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✓
	Delayed Actuation (P-DA)	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗
	Prevented Actuation (P-PA)	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Direct Consequences (DC)	Financial (DC-F)	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓
	Vocational (DC-V)	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗
	Invasion of privacy (DC-P)	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
	Loss of Control (DC-LC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Inconvenience (DC-I)	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓
User Experience (UX)	Instantly Noticeable (UX-N1)	✗	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓
	Noticeable over time (UX-N2)	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
	Not noticeable (UX-NN)	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗
Emotional (E)	Appraisal (E-A)	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓
	Action Tendencies (E-AT)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Bodily Symptoms (E-B)	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓
	Expression (E-EX)	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗
	Subjective feeling (E-SF)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

associated with each threat. Building on the previous Threat Identification step, we established a set of attack patterns corresponding to each identified threat. By utilizing the CAPEC database, the vulnerabilities linked to each threat can be systematically identified.

Table 5 outlines the vulnerabilities associated with the top five threats of the selected smart camera in order to understand the potential flaws that could compromise a system. For instance, the *Process Discovery* threat is associated with the *Process Footprinting* attack pattern (CAPEC-ID 573). As indicated in Table 6, the vulnerabilities related to the *Process Footprinting* attack pattern include the CWE-200 (see Section 2.2 for the CAPEC details). Therefore, the vulnerabilities corresponding to the *Process Discovery* threat are represented by the CWE-200. Similarly, the *Dynamic Linker Hijacking* threat maps to two attack patterns: *Subverting Environment Variable Values* (CAPEC-ID 13) and *Inclusion of Code in Existing Process* (CAPEC-ID 640). According to Table 6, the vulnerabilities for the *Subverting Environment Variable Values* attack pattern include the CWE-15, CWE-20, CWE-73, CWE-74, CWE-200, CWE-285, CWE-302 and CWE-353. The vulnerabilities for the *Inclusion of Code in Existing Process* attack pattern include the CWE-114 and CWE-829. As a result, the vulnerabilities associated with the *Dynamic Linker Hijacking* threat are an aggregation of these identified weaknesses.

5.4. Impact assessment

After identifying the total vulnerabilities within the smart home, the next step is to evaluate the impact of threats on each asset, which we undertake in this section. To maintain clarity and avoid redundancy, we will focus on presenting the impact of a single threat—the Rootkit threat on the smart camera. However, it is important to note that a similar assessment has been conducted for all threats across all assets. Following the methodology outlined in Section 4.4, the process involves three steps: (*i*) determining the criticality of each factor to the smart camera, (*ii*) assessing the impact of the Rootkit threat on the smart camera for each factor, and (*iii*) calculating the total impact of the Rootkit threat on the smart camera.

The first step is to determine the criticality of each factor to the smart camera. According to Eq. (3), the criticality of a factor is calculated as the sum of the subfactors critical to the asset divided by the total number of subfactors for that factor. From Table 7, we observe

Table 8
Calculated criticalities of assets' factors.

Assets	Criticalities (C)				
	Cyber (C)	Physical (P)	Direct Consequences (DC)	User Experience (UX)	Emotional (E)
Smart camera	0.75	0.4	0.8	0.33	0.4
Smart doorbell	0.25	0.4	0.2	0.33	0.4
Smart alarm	0.25	0.4	0.4	0.33	0.4
Smart TV	0.75	0.4	0.8	0.66	1
Smart light switch	0.25	0.6	0.4	0.33	0.4
Smart water leak sensor	0.5	0.4	0.4	0.33	0.4
Smart irrigation controller	0.5	0.4	0.4	0.33	0.4
Smart moisture sensor	0.25	0.4	0.4	0.33	0.4
Smart refrigerator	0.5	0	0.6	0.33	0.6
Smart washing machine	0.25	0	0.4	0.33	0.4
Smart speaker	1	0.2	0.4	0.66	0.8
Smart oven	0.75	0.6	0.6	0.33	0.8

Table 9
Weights of threats to factors for smart camera.

Threats	Weights (W)				
	Cyber (C)	Physical (P)	Direct Consequences (DC)	User Experience (UX)	Emotional (E)
Dynamic Linker Hikacking	0.4	0.2	0.2	0.1	0.1
Impair Command History Logging	0.4	0.2	0.2	0.1	0.1
Brute Force	0.2	0.1	0.2	0.1	0.4
Process Discovery	0.4	0.1	0.3	0	0.2
Rootkit	0.4	0.1	0.4	0	0.1

that only the Confidentiality, Integrity, and Availability subfactors are critical for the smart camera. In addition, the Cyber factor has four subfactors in total. Therefore, the criticality of the Cyber factor is $\frac{3}{4} = 0.75$. Similarly, the criticality of the other factors for the Smart Camera are as follows: the Physical factor is 0.4; the Direct Consequences factor is 0.8; the User Experience factor is 0.33; and the Emotional factor is 0.4. Table 8 presents the calculated criticalities of factors for the assets.

The second step is to assess the impact of the Rootkit threat on the smart camera for each factor. According to Eq. (4), the impact of a threat on an asset due to a specific factor is the product of the threat's weight for that factor, the existence of the threat for that factor, and the criticality of the factor to the asset. To ensure a realistic evaluation, we assume that the threat is present in all factors; hence, the existence of the threat for each factor equals 1. From the last line of Table 9, we obtain the weights of the Rootkit threat for each factor concerning the smart camera. Consequently, the impact of the Rootkit threat on the Cyber factor is $0.4 \times 1 \times 0.75 = 0.3$. Similarly, the impacts of the Rootkit threat on other factors are as follows: the Physical factor impact is 0.04; the Direct Consequences factor impact is 0.32; the User Experience factor impact is 0; and the Emotional factor impact is 0.04. Table 10 presents the calculated impacts of the five threats on the Smart Camera for each factor.

The third step is to calculate the total impact of the Rootkit threat on the smart camera. According to Eq. (5), the total impact of a threat on an asset is the sum of the impacts of the threat on the asset for all factors. Thus, the total impact of the Rootkit threat on the smart camera is $0.3 + 0.04 + 0.32 + 0 + 0.04 = 0.7$. Similarly, we compute the impacts of other threats on the smart camera: the impact of the Dynamic Linker Hijacking threat is 0.577, the impact of the Impair Command History Logging threat is 0.613, the impact of the Brute Force threat is 0.543, and the impact of the Process Discovery threat is 0.66. Table 11 presents the total impacts of the top five threats on the smart camera.

5.5. Risk measurement and analysis

Having identified the likelihood of threats and the impacts of threats, the following step is to measure and analyze the risk. In this section, firstly, we find the risk of a threat to an asset, then we find the risk of asset and after we find the risk of smart home. Secondly, we analyze the findings of risk measurements. We consider the scenario where the asset is the smart camera and the threat is the Rootkit.

5.5.1. Risk measurement

The first step involves determining the risk of a threat to an asset. According to Eq. (7), the risk of a threat to an asset is calculated as the product of the likelihood of the threat and its impact. Based on the measurements of the threats' likelihood (Table 4) and their corresponding impacts (Table 11), the risk of a Rootkit threat to the smart camera is calculated as $0.5 \times 0.7 = 0.35$. Similarly, the risk of other threats to the smart camera is determined: the risk of Dynamic Linker Hijacking is 0.2885; the risk of the Impair Command History Logging threat is 0.4597; the risk of a Brute Force threat is 0.2715; and the risk of a Process Discovery threat is 0.165.

The second step is to assess the overall risk of an asset. According to Eq. (8), the risk of an asset is the sum of the risks posed by all threats to that asset. For the smart camera, the sum of all threat risks, not only the top five, is calculated as 34.1921. To normalize this risk, the maximum possible risk for the smart camera must first be determined. This is done by considering each threat's highest possible impact (i.e., 1) and the maximum likelihood (i.e., 0.75). Consequently, the maximum possible risk for each threat of the smart camera is $1 \times 0.75 = 0.75$. According to Eq. (9), the maximum possible risk for the smart camera is $95 \times 0.75 = 71.25$ (where 95 represents the maximum number of threats). Finally, according to Eq. (10), the normalized risk of the smart camera is calculated as $\frac{34.1921 \times 100}{71.25} = 47.9889$. Table 12 presents the calculated total risks per asset and their normalized values (see Table 3).

The third step is to assess the risk of the smart home. According to Eq. (11), the risk of a smart home is the sum of all assets' normalized risks. Therefore, the risk of the smart home is the sum of 47.9889, 18.3785, 23.7399, 53.6145, 11.2444, 12.1073, 12.1073, 10.0809, 9.4096, 5.7692, 12.7904, and 12.9654, which totals 230.1963. To normalize the risk of the smart home, the maximum possible risk must first be calculated, assuming that each asset is at its highest possible risk. This maximum possible risk is determined by assuming that each asset could reach a normalized risk of 100. According to Eq. (12), the maximum possible risk for the smart home is calculated as $12 \times 100 = 1200$, where 12 is the total number of assets in the

Table 10
Impacts of threats to factors for smart camera.

Threats	Impacts (I)				
	Cyber (C)	Physical (P)	Direct Consequences (DC)	User Experience (UX)	Emotional (E)
Dynamic Linker Hikacking	0.3	0.08	0.16	0.033	0.004
Impair Command History Logging	0.3	0.08	0.16	0.033	0.04
Brute Force	0.15	0.04	0.16	0.033	0.16
Process Discovery	0.3	0.04	0.24	0	0.08
Rootkit	0.3	0.04	0.32	0	0.04

Table 11
Total impacts of five threats for smart camera.

Threats	Total impacts
Dynamic Linker Hikacking	0.577
Impair Command History Logging	0.613
Brute Force	0.543
Process Discovery	0.66
Rootkit	0.7

Table 12
Risk per asset.

Asset	Risk	Normalized risk
Smart camera	34.1921	47.9889
Smart doorbell	13.0947	18.3785
Smart alarm	16.9147	23.7399
Smart TV	38.2003	53.6145
Smart light switch	8.0117	11.2444
Smart water leak sensor	8.6265	12.1073
Smart irrigation controller	8.6265	12.1073
Smart moisture sensor	7.1827	10.0809
Smart refrigerator	6.7044	9.4096
Smart washing machine	4.1106	5.7692
Smart speaker	9.1132	12.7904
Smart oven	9.2379	12.9654

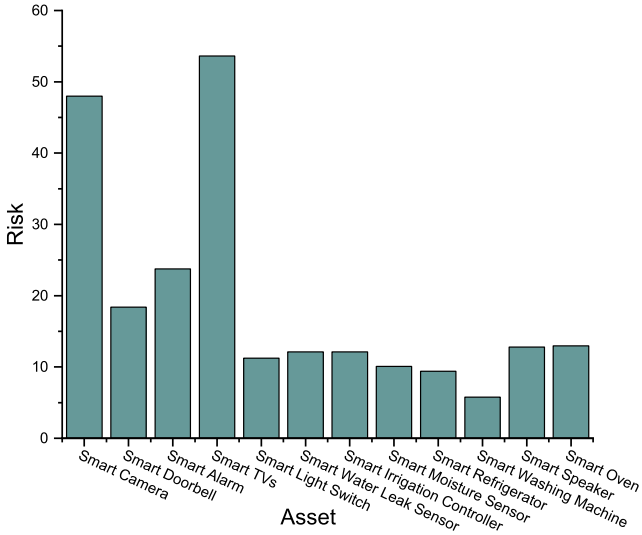

Fig. 3. Normalized risk per asset.

smart home. Next, to normalize the total risk of the smart home, the calculated risk is divided by the maximum possible risk and then multiplied by 100 to convert it into a percentage scale ranging from 0 to 100. According to Eq. (13), the normalized risk of the examined smart home is $\frac{230.1963}{1200} \times 100 = 19.1830$. Therefore, based on qualitative form of Section 4.5 the examined smart home poses a low risk.

5.5.2. Risk analysis

In this section, we present a comprehensive analysis of the risk measurements and describe the central tendency of risk across smart home assets, focusing on the median risk. This analysis is crucial in cyber risk assessment, as it emphasizes the central value of risk associated with these assets, thereby minimizing the influence of outliers that could distort the overall risk perception for smart homes.

Fig. 3 illustrates the risks associated with various smart home assets. Each column represents a specific asset, highlighting its corresponding risk value. The analysis uncovers a wide range of risk levels among different assets. Notably, the smart TV exhibits the highest risk, with a value of 53.6145, closely followed by the smart camera at 47.9889. The smart alarm and smart doorbell also demonstrate significant risk levels, with values of 23.7399 and 18.3785, respectively. These assets, categorized under the Electronics and Controllers class, collectively exhibit an average risk value of 35.9304. In contrast, assets within the Sensor class display substantially lower risk levels. Specifically, the smart light switch, smart water leak sensor, smart irrigation controller, and smart moisture sensor have risk values of 11.2444, 12.1073, 12.1073, and 10.0809, respectively, leading to an average risk value of 11.3849 for this class. The Gadgets and Appliances category, which includes the smart refrigerator, smart washing machine, smart speaker, and smart oven, presents the lowest risk levels among all asset categories. The risk values for these assets are 9.4096, 5.7692, 12.7904, and 12.9654, respectively, resulting in an average risk value of 10.2336 for this category. This assessment highlights a significant disparity in cyber risk across different classes of smart home assets, with the Electronics and Controllers category being the most vulnerable, followed by Sensors, and lastly, Gadgets and Appliances.

On top of that, Fig. 4 details the distribution of cyber risks across smart home assets, emphasizing the distinct median risk values within each asset class. This underscores the variability in vulnerability among different types of devices. Within the Electronics and Controllers class, the smart TV exhibits the highest median risk of 0.41, indicating substantial exposure to cyber threats. The smart camera, smart doorbell, and smart alarm follow with median risks of 0.13, 0.17, and 0.35, respectively. The Sensors class, which includes the smart light switch, smart water leak sensor, smart irrigation controller, and smart moisture sensor, demonstrates a lower average median risk of 0.197525. Gadgets & Appliances, show the lowest average median risk at 0.2367. Overall, the average of the median risks across all assets is 0.2331.

5.6. Scenarios

In this section, we evaluate the proposed cyber risk assessment methodology for smart home electronic devices in two distinct scenarios, each highlighting different aspects of cyber risks within smart homes. Each scenario includes a selection of devices chosen for their specific functions and the unique vulnerabilities they introduce.

Security-Centric Smart Home. In the first scenario, the focus is on devices integral to home security and user interaction. The selected devices are a smart camera, a smart doorbell, a smart alarm, a smart light switch, and a smart speaker. These devices are often interconnected, meaning a breach in one can lead to vulnerabilities in others. They handle sensitive data such as audio, video, and access controls, which are crucial for personal privacy and physical safety. Security devices

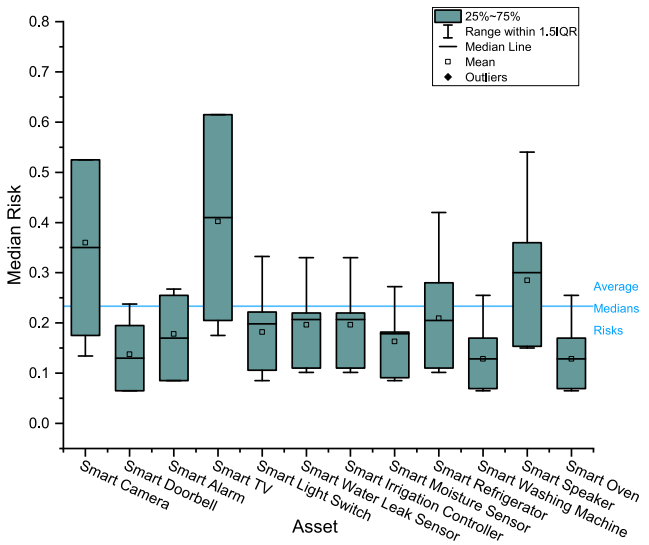

Fig. 4. Median risk per asset.

are attractive targets for attackers due to the potential impact of their compromise. The smart camera monitors the interior and exterior of the home. If compromised, it can lead to privacy breaches, unauthorized surveillance, and insights into the homeowner's daily routines. The smart doorbell, equipped with video and audio capabilities, allows homeowners to monitor and communicate with visitors. A hacked doorbell can grant attackers visual and auditory access to the home's entrance, potentially facilitating unauthorized entry. The smart alarm acts as the first line of defense against intrusions. If an attacker disables or manipulates the alarm system, it can render the home vulnerable to physical break-ins without immediate detection. The smart light switch controls lighting remotely and can be programmed for specific patterns. If compromised, it can reveal occupancy patterns or be used to simulate occupancy, misleading the homeowner or neighbors. The smart speaker, often connected to voice assistants, controls various smart devices and can access personal information. Unauthorized access can lead to control over other devices and eavesdropping on conversations. Lastly, the smart TV provides entertainment and often includes internet connectivity for streaming services, browsing, and apps. If compromised, it can be used to access personal accounts, display unwanted content, or even activate the built-in camera and microphone to spy on occupants.

Utility Management Smart Home. The second scenario centers around devices that manage utilities and household operations. The selected devices are a smart refrigerator, a smart washing machine, a smart oven, a smart irrigation controller, a smart moisture sensor, and a smart water leak sensor. These devices directly impact water and energy consumption, making them critical for sustainability and cost management. Attacks can cause significant inconvenience, financial loss, or property damage without necessarily compromising personal data. Misuse can lead to hazardous conditions, such as fire hazards from the oven or mold growth from over-irrigation. The smart refrigerator keeps track of inventory, suggests shopping lists, and can order groceries. A breach can expose dietary habits, shopping patterns, and personal schedules. The smart washing machine allows remote operation and maintenance monitoring. Compromise can lead to unauthorized use, increased utility bills, or even physical damage due to improper operation. The smart oven enables remote cooking and temperature control. A hacked oven poses safety risks like fire hazards or energy wastage. The smart irrigation controller manages garden watering schedules based on weather and soil conditions. Unauthorized access can result in overwatering or underwatering, affecting utility costs and plant health. The smart moisture sensor works with the irrigation system to optimize watering. If manipulated, it can send false readings, leading to inefficient water usage. The smart water leak sensor detects leaks to prevent water damage. A compromised sensor might fail to alert homeowners of real leaks or generate false alarms.

Evaluation of CRASHED. Using the proposed methodology, the total risk for each scenario is calculated. The Security-Centric Smart Home has a total risk of 34.3286, whereas the Utility Management Smart Home has an overall risk of 26.2669. The findings indicate that the cyber risk in Security-Centric Smart Home scenarios is greater than in Utility Management Smart Home scenarios. The higher total risk in the first scenario can be attributed to several factors. Smart cameras, smart doorbells, smart alarms, smart speakers, and smart TVs are devices that handle highly sensitive personal information, significantly impacting our privacy and physical security. Compromising any of these elements can lead to detrimental consequences, as attackers may gain access to live video feeds, private discussions, and, most critically, security systems. A smart TV with access to personal accounts poses an elevated danger, serving as a new entry point for network breaches. Conversely, although the Utility Management Smart Home scenario presents considerable risks to operational integrity and resource management, its overall implications are less severe. Although these technologies may also entail drawbacks resulting in financial losses, discomfort, and property damage, their immediate and direct effects on human safety and privacy are less significant than those of the devices in the initial scenario.

6. Discussion

This section critically evaluates the proposed cyber risk assessment methodology for smart homes, focusing on its practical implications and areas for potential refinement. First, we discuss the limitations of the current approach. We then outline future research directions to improve the methodology, enhancing its robustness and adaptability to address the continuously evolving cyber threats in smart home environments. Finally we propose other domains in which *CRASHED* can be utilized.

6.1. Limitations

Despite the notable benefits of the proposed methodology, it is important to recognize certain limitations that require attention. The *CRASHED* methodology primarily focuses on assessing cyber risks at the individual device level, providing detailed analyses of specific vulnerabilities and threats associated with each device. However, this device-centric approach may not fully account for the broader risks arising from the interconnected nature of smart home ecosystems. In real-world smart homes, devices are often interdependent, meaning that a vulnerability in one device could potentially trigger cascading effects across others. To address this, incorporating a more holistic approach that considers device interactions and interdependencies could enable *CRASHED* to assess overall cyber risks within smart homes comprehensively. This could be achieved by developing models that simulate cascading effects and interconnected risks, which is essential for understanding the full impact of vulnerabilities in complex smart home environments.

Additionally, another limitation arises from the assumption of uniform network conditions within the smart home environment, simplifying cyber risk analysis by considering a consistent network setup. However, this assumption may not accurately reflect the variability in network configurations in real-world smart homes. Factors such as network architecture, signal strength, bandwidth availability, and external interferences can vary significantly between households. These variations can influence smart devices' performance, security, and vulnerability. For example, a poorly segmented network might expose

more devices to potential threats, while a high-bandwidth environment could support more sophisticated attacks. To address these challenges, adapting *CRASHED* to account for diverse and dynamic network conditions would enhance the accuracy and relevance of cyber risk assessments across different smart home scenarios.

To maintain conceptual clarity and focus, it is critical to note that this article centers exclusively on the cyber risk assessment process as specified by the *CRASHED* methodology. While the study offers a comprehensive examination of the identification, analysis, and evaluation of cyber risks within smart home environments, it does not address, detail, or implement any mitigation plans. The principal objective is to establish a robust framework for understanding and systematically evaluating cyber risks in smart homes.

The final limitation concerns the inherent nature of MITRE and CAPEC frameworks. As technology evolves, so do the tactics, techniques, and procedures (TTPs) employed by cybercriminals, making it increasingly challenging to predict potential attacks. Threat actors continuously discover new vulnerabilities and rapidly develop novel exploitation methods to target these weaknesses. Consequently, a methodology that relies solely on current threat models may quickly become outdated, as it may need to account for emerging threats or newly identified vulnerabilities. Furthermore, CAPEC may not always reflect the most up-to-date attack patterns due to its reliance on documented patterns, leading to potential gaps in assessing newly developed or rapidly evolving threats. This limitation could be mitigated by integrating real-time threat intelligence feeds and emerging attack frameworks into the *CRASHED* methodology.

Despite these limitations, the proposed cyber risk assessment methodology remains valuable for enhancing cyber risk assessment practices in smart homes. By acknowledging and proactively addressing these constraints, researchers and practitioners can enhance the methodology's applicability across diverse smart home contexts and improve its resilience against an evolving cyber threat landscape.

6.2. Future research directions

Several promising research opportunities could significantly advance the *CRASHED* methodology for assessing cyber risks in smart homes. One primary area of focus should be exploring factors and subfactors that influence the impact of threats on smart home assets. Through comprehensive research and analysis, new factors and subfactors could be identified that better capture the complexities of cyber threats. Conversely, existing elements that are less relevant might be refined or removed. This continuous refinement process will enhance the precision and effectiveness of the *CRASHED* methodology in evaluating cyber risks within the diverse and rapidly evolving landscape of smart home environments.

To ensure the reliability and applicability of the proposed methodology, future research must include rigorous evaluations, mainly through focused group studies. Engaging cybersecurity professionals, smart home technology manufacturers, and other key stakeholders will provide valuable insights into the methodology's effectiveness. This collaborative and iterative approach will help identify further improvement and refinement areas. Incorporating diverse perspectives will enhance the credibility and practical application of the *CRASHED* methodology in real-world smart home settings, ensuring that it meets the practical needs and challenges inherent in dynamic and complex smart home ecosystems.

In conclusion, future research directions include refining the critical factors and subfactors involved in the impact assessment phase and rigorous evaluation through focused groups. By pursuing these research avenues, we aim to enhance the effectiveness of our methodology and establish it as a valuable tool in the field of cyber risk assessment for smart homes.

6.3. Beyond smart homes

The need for robust risk assessment methodologies grows as interconnected systems become increasingly prevalent. While *CRASHED* is primarily designed to address cybersecurity risks in smart home environments, it can also be applied across other domains. In the following, we explore how *CRASHED* can extend beyond the confines of smart homes to provide comprehensive cybersecurity solutions in critical and emerging fields.

Smart Cities. Smart cities integrate various connected devices, including traffic management systems, public safety solutions, and energy-efficient infrastructure. These systems are vital for efficient urban living but are highly vulnerable to cyberattacks due to their interconnectivity and reliance on IoT technologies. *CRASHED* can be utilized to assess the security risks in these environments, mainly focusing on smart streetlights, public Wi-Fi systems, and sensors used in public transportation. By applying the *CRASHED* methodology, city officials can identify vulnerabilities that could be exploited to disrupt city functions or compromise the safety and privacy of citizens. Moreover, *CRASHED*'s ability to factor in threats' physical and systemic impact can ensure that smart cities are resilient against cyberattacks that could cause widespread disruption.

Energy Infrastructure. In the energy sector, particularly within smart grids and renewable energy systems, *CRASHED* can be adapted to assess the risks associated with the increasing use of IoT devices for monitoring and controlling energy production and distribution. The interconnectedness of smart meters, grid management systems, and power generation units makes them prime targets for cyberattacks that could lead to widespread power outages or manipulation of energy consumption data. *CRASHED* provides a robust solution to evaluate the security posture of these critical infrastructures, leveraging the MITRE ATT&CK and CAPEC frameworks to identify potential threats and vulnerabilities in energy infrastructure systems. This approach can help energy providers enhance their cybersecurity measures, ensuring the continuity and security of energy supplies.

Industrial IoT. The Industrial Internet of Things (IIoT) encompasses many interconnected devices and systems within industrial sectors, such as manufacturing, logistics, agriculture, and automotive. These devices monitor, control, and optimize industrial processes, making operations more efficient and exposing them to significant cyber threats. *CRASHED* can be applied to assess the cybersecurity risks within IIoT environments, where critical systems such as sensors, actuators, and industrial controllers are interconnected. The methodology helps identify vulnerabilities in industrial control systems and evaluates the risk of cyberattacks that could disrupt operations, damage equipment, or even endanger human lives. By leveraging frameworks like MITRE ATT&CK and CAPEC, *CRASHED* provides a detailed analysis of potential threats and helps industrial organizations strengthen their security posture, ensuring the integrity and resilience of critical infrastructure.

Healthcare. In the healthcare sector, the proliferation of IoT devices such as connected medical equipment, wearable health monitors, and smart hospital systems has dramatically improved patient care. However, it also introduces a range of cybersecurity risks that could have life-threatening consequences. Medical devices, electronic health record systems, and hospital networks are prime targets for cyberattacks, which could lead to the theft of sensitive patient data or disruption of critical medical services. *CRASHED* can be employed to perform a comprehensive risk assessment of these interconnected systems, identifying potential vulnerabilities in both hardware and software. With *CRASHED*, healthcare institutions can mitigate risks associated with data breaches, ransomware attacks, and unauthorized access to medical devices, ultimately safeguarding patients and operational continuity.

Maritime. As maritime systems become increasingly digitized through the interconnectivity of navigation, communication, and cargo systems,

they inherit cybersecurity challenges like those found in smart homes. These challenges, involving connected devices, inconsistent cybersecurity frameworks, and potential data loss, have been well documented in the literature [44,45]. *CRASHED* can leverage frameworks such as MITRE ATT&CK, CAPEC, and CWE to identify threats requiring assessment for maritime assets, including bridge navigation systems, engine control units, and satellite communication systems. Moreover, the maritime environment frequently relies on legacy systems that must interface with newer digital technologies, making it susceptible to cyberattacks. With its structured approach to threat identification, vulnerability assessment, and risk quantification, *CRASHED* can also support the evaluation of Industrial Control Systems (ICS) and Operational Technology (OT) onboard ships and at port facilities. By considering the potential cascading impact cyber threats could have on interdependent onboard and shore-based maritime systems, *CRASHED* enables maritime cybersecurity practitioners to prioritize risk mitigation efforts, reflecting the critical nature of maritime and aeronautical operations. Finally, by adopting *CRASHED* in the maritime domain, stakeholders gain deeper insights into emerging risks, enhance incident response and preparedness, and proactively safeguard vessels, cargo, and critical maritime infrastructure from an evolving threat landscape.

7. Related work

At the same time that the field of smart home technology is expanding rapidly, a substantial volume of literature investigates various aspects of cyber risk assessment. The majority of previous works have focused on concerns regarding data privacy and cybersecurity risks. Nevertheless, it is still abundantly clear that a comprehensive and holistic approach is required.

Bugeja et al. [46] proposes the PRASH framework for modeling and analyzing the privacy risks of smart homes, comprising three modules: a system model, a threat model, and a set of privacy metrics. This framework allows for early identification of threats, better planning for risk management scenarios, and mitigation of potential impacts caused by attacks before they compromise the lives of residents. By providing an executable version of the smart home system configuration, PRASH aids in identifying potential attack paths and mitigating the impacts of those attacks, contributing to the preservation of residents' privacy rights in the face of emerging challenges affecting smart homes. In the risk calculation phase, this work employs the CVSS and NVD vulnerability databases and utilizes the DREAD methodology to assess the risks.

Flores et al. [47] proposes a risk assessment model for a smart home IoT utilizing a Bayesian network developed based on an attack graph, which comprehensively represents probable attack vectors. The parameters of the Bayesian network are calculated using the maximum likelihood approach. This estimation process uses attack simulation data derived from five distinct scenarios. These scenarios focus mainly on Denial of Service (DoS) and Man-in-the-Middle (MitM) assaults, specifically targeting automation devices with comparatively lower levels of individual security. In the risk calculation phase, this work employs the CVSS Vulnerability database.

Pturgess et al. [48] examine the difficulties associated with evaluating privacy concerns in smart homes, emphasizing the complex structure of smart gadgets, the extensive and diverse range of potential threats, and the issues in assigning value to personal data. In order to address these difficulties, the authors bring up a capability-oriented methodology that simplifies the smart home ecosystem to its data-gathering capabilities and evaluates privacy risks by considering the information disclosed by the user. This approach aims to develop a model that is adaptable to different systems and can accommodate the dynamic nature of smart homes.

Wang et al. [49] proposes a privacy risk assessment methodology for smart home systems, which integrates the system theoretic process analysis–failure mode and effect analysis (STPA–FMEA) approach. The methodology considers the complex dynamics and interplay among the user, environment, and smart house products to comprehensively evaluate privacy risks. The STPA-FMEA methodology can comprehensively identify privacy risk scenarios within a smart home system, as well as the insecurity restrictions present in the hierarchical control structure of this system. The risk control strategies derived from the STPA-FMEA analysis exhibit a high potential for effectively mitigating the privacy risk associated with the smart home system.

Park et al. [50] presents a novel framework for assessing the security risks associated with information leakage in IoT-based smart homes, focusing on a situational awareness perspective. The authors propose a hierarchical risk assessment system that considers both the cyber and physical layers of smart homes. The proposed framework utilizes work based on Factor Analysis of Information Risk (FAIR) and clustering method. Through situational awareness, the framework tries to present a view of security threats that is both more contemporary and contextualized. This goes beyond static evaluations and takes into consideration the ever-changing nature of risk in surroundings that are interconnected among themselves. In the risk calculation phase, this work employs the CVSS Vulnerability database.

Arat and Akleylek [51] proposed an innovative methodology that integrates a three-phase risk assessment framework encompassing graph construction, attack path detection, and subsequent filtering to offer a more granular and efficient evaluation of vulnerabilities and risks in IoT-based networks. Providing a more granular and efficient evaluation of vulnerabilities and hazards in networks that are formed on the IoT is the goal of this methodology, which aims to do this. Their approach is an example of a substantial advancement in the field because it employs a modified version of the Depth First Search (DFS) algorithm for path discovery and uses CVSS metrics for risk computation. The proposed framework is considered in the case of a smart home that is a given IoT-based system. This work employs the CVSS, NVD, and CVE vulnerability databases in the risk calculation phase.

Collen and Nijdam [52] focused on the risk assessment for smart home environments to incorporate multiple types of IoT devices. This work presents a dynamic risk assessment framework to automate the detection of ongoing assaults and the evaluation of the probability of risks related to such assaults. The proposed framework uses risk assessment by concentrating on the attacks and the relationship between them. Furthermore, the framework emphasizes interoperability with external reporting by bringing forward a specified Application Programming Interface (API) for anomaly reports. This simplifies anomaly reporting, making the framework autonomous and applicable to other dynamic environments. Finally, the proposed framework proposes solutions to mitigate risks when completely automating decision-making is impossible. In the risk calculation phase, this work integrates weighted formulas and utilizes the DRAF methodology to assess the risks.

A novel complete privacy threat analysis and risk management strategy is proposed by Alalade et al. [53]. This approach is distinguished because it considers the privacy concerns of both users and devices concerning their data. Also, the work is groundbreaking because it incorporates the LINDDUN PRO privacy engineering (PE) framework into the SH systems domain. This represents a pioneering effort to holistically address the issue of user and device data privacy using a comprehensive privacy threat analysis (PTA), a privacy impact assessment (PIA), and the identification of appropriate privacy enhancement technologies (PETs).

Parsons et al. [54] present a novel method for measuring the sensitivity of home environments to IoT hazards by focusing on human elements. The Smart Home Conduct and Attitude Risk Model (SHBRAM) emphasizes the significance of user conduct and attitudes in the context of smart home security. This concept is notable for combining risk management strategies with an end-user emphasis, which implies that an individual's behaviors and predispositions significantly impact the IoT's security in the home. Their work demonstrates the application of their technique in real-world conditions using a comprehensive case

Table 13
Comparison of different approaches.

Works	Contribution	Security issues	Privacy issues	Vulnerabilities databases @ Risk calculation	Weighted formulas @ Risk calculation	Methodologies
Bugeja et al. [46]	Framework	✗	✓	✓	✗	DREAD
Flores et al. [47]	Model	✓	✗	✓	✗	Bayesian
Pturgess et al. [48]	Model	✗	✓	✗	✗	n/a
Wang et al. [49]	Method	✗	✓	✗	✗	STPA-FMEA
Park et al. [50]	Framework	✗	✓	✓	✗	FAIR
Arat and Akleylek [51]	Method	✓	✗	✓	✗	n/a
Collen and Nijdam [52]	Framework	✓	✓	✗	✓	n/a
Alalade et al. [53]	Methodology	✗	✓	✗	✗	LINDDUN PRO
Parsons et al. [54]	Model	✓	✓	✗	✗	n/a
Pandey et al. [55]	Model	✓	✗	✗	✗	Negative to Positive
Wongvises et al. [56]	Method	✓	✗	✓	✗	n/a
Jacobsson et al. [57]	Empirical evaluation	✓	✓	✓	✗	ISRA
Ali and Awad [33]	Methodology	✓	✗	✓	✗	OCTAVE Allegro
CRASHED	Methodology	✓	✓	✓	✓	MITRE ATT&CK

study, highlighting the significance of user education, awareness, and proactive action in the risk mitigation process.

Pandey et al. [55] provide a risk assessment model generated from the Negative to Positive method. Automating the process of threat-based risk assessment, specifically tailored to the configurations of smart homes, is the objective of the model to achieve this goal. Using threat-triggered evaluation scenarios that have been built, the utilization of the calculation model is explained and demonstrated. The construction of these scenarios was accomplished by utilizing a technology that consisted of analyzing historical evidence of data exchange within the framework of smart homes.

Wongvises et al. [56] propose a method for quantifying security risks that establishes a certain smart house's security by evaluating smart home devices. In turn, this makes it possible to assess a smart house's security level. Fault Tree Analysis (FTA), which is the methodology that is typically applied in systems that are regarded to be mission-critical, serves as the foundation for their method. After developing a vulnerability tree of a smart home, the authors applied the inclusion-exclusion law of probability to it in order to ascertain the amount of risk. This work employs the CVSS, NVD, and CVE vulnerability databases in the risk calculation phase.

A detailed risk assessment of a smart home automation system was carried out by Jacobsson et al. [57]. The findings of this study highlighted the importance of incorporating security and privacy concerns into the design phase of a smart home automation system. The Information Security Risk Analysis (ISRA) method is utilized to assess the vulnerabilities and threats associated with the system, the likelihood that they will occur, and the potential consequences they may have. The results indicate that the high risks are associated with either the human factor or the software components of the system, pointing out that the risks derived from the human factor would require additional consideration. In the risk calculation phase, this work employs the CVE Vulnerability database.

Ali and Awad [33] discuss the importance of conducting a comprehensive security risk assessment for IoT-based smart homes, highlighting the need to consider both cyber and physical security aspects. They made use of the OCTAVE Allegro approach, and they suggested a number of different countermeasures in order to reduce the detected security risks and threats.

Table 13 compares the related work with the *CRASHED*. Works that have a checkmark in the *Security Issues* column indicate that their proposed risk assessments include the detection of weaknesses in the smart home, prospective threats (such as hackers or malware), and the impact of these threats making their way into the smart home. Works that have a checkmark in the *Privacy Issues* column indicate that their proposed risk assessment includes the analysis of data life cycle management techniques, permission processes, and data minimization practices. Works with checkmarks in both columns, *Security Issues* and *Privacy Issues*, including the set of them. The third and fourth columns pertain to the characteristics involved in calculating risk. Works with checkmarks in the *Vulnerability Databases @ Risk Calculation* column demonstrate their use of vulnerability databases for risk calculation, while those with checkmarks in the *Weighted Formulas @ Risk Calculation* demonstrate their use of weights for risk measurement. Based on the Table 13, a significant gap exists in the cyber risk assessment for smart homes, as the majority of works do not utilize these characteristics. Lastly, the *Methodologies/Frameworks* column indicates risk methodologies or frameworks that contributed to the process of the proposed risk assessment. Consequently, *CRASHED* is the sole cyber risk assessment methodology that leverages MITRE ATT&CK and CAPEC frameworks and addresses security and privacy issues by basing the risk calculation on vulnerability bases and using a weighting formula.

8. Conclusion

The increasing integration of smart home devices into daily life has brought about unparalleled convenience, yet it has also introduced significant cybersecurity challenges that demand immediate attention. This article introduced *CRASHED*, a comprehensive cyber risk assessment methodology specifically designed to address the unique vulnerabilities of smart home environments. By integrating the MITRE ATT&CK and CAPEC frameworks, *CRASHED* provides a robust mechanism for identifying, analyzing, and quantifying the risks posed by cyber threats. The methodology's emphasis on device profiling and the holistic assessment of threats and vulnerabilities offers a more precise evaluation of potential risks than traditional approaches. The case study presented validates the effectiveness of *CRASHED* in identifying critical threats and formulating strategies to mitigate potential impacts on smart homes. As smart home adoption grows, the need for tailored cybersecurity solutions becomes increasingly critical. *CRASHED* fills this gap and sets a new standard for cyber risk assessment in smart home ecosystems, paving the way for more secure and resilient digital living environments.

CRediT authorship contribution statement

Georgios Paparis: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Apostolis Zarras:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Aristeidis Farao:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation,

Conceptualization. **Christos Xenakis:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization.

Research data/code availability

The source code is available at https://github.com/UniPiSSL/CRASHED.

Compliance with ethical standards

This article does not contain any studies with human participants or animals performed by any of the authors.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work the authors used Grammarly in order to improve language and readability. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Declaration of competing interest

The authors declare no conflict of interest.

Acknowledgments

This research has received funding from European Commission's Horizon Europe and Horizon 2020 research and innovation programs under grant agreements No. 101082440 (CHRISS); No. 101095634 (ENTRUST); No. 101092702 (OASEES); No. 101120962 (RESCALE).

Source code availability

The source code is available at https://github.com/UniPiSSL/CRASHED.

References

[1] Grand View Research. Smart home market size & trends. 2023, https://rb.gy/w6xtl8.
[2] Kor A-L, Pattinson C, Yanovsky M, Kharchenko V. IoT-enabled smart living. Technol Smart Futur 2018;3–28.
[3] Marques G, Saini J, Dutta M. IoT enabled computer-aided systems for smart buildings. Springer; 2023.
[4] Hammi B, Zeadally S, Khatoun R, Nebhen J. Survey on smart homes: Vulnerabilities, risks, and countermeasures. Comput Secur 2022;117:102677.
[5] Report ZE. 65% of US households impacted by cybersecurity in the home security industry statistics. 2024, https://rb.gy/yphuhw.
[6] New York Times. Somebody's watching: Hackers breach ring home security cameras. 2024, https://rb.gy/o1ajl0.
[7] News N. Stranger hacks into baby monitor, tells child, 'I love you'. 2019, https://rb.gy/arfaem.
[8] Nord VPN. Hacker terrorizes family by hijacking baby monitor. 2018, https://rb.gy/vts680.
[9] Forbes. Hackers use ddos attack to cut heat to apartments. 2026, https://rb.gy/8vtmdw.
[10] Pami S, Dai Y, Tan SRX, Roy N, Han J. Spying with your robot vacuum cleaner: Eavesdropping via lidar sensors. In: Proceedings of the 18th conference on embedded networked sensor systems. 2020, p. 354–67.
[11] Kaspersky. Xiaomi mi robot vacuum cleaner hacked. 2018, https://rb.gy/gfeaka.
[12] Görmüş S, Aydın H, Ulutaş G. Security for the internet of things: A survey of existing mechanisms, protocols and open research issues. J Fac Eng Archit Gazi Univ 2018;33(4):1247–72.
[13] Yamauchi M, Ohsita Y, Murata M, Ueda K, Kato Y. Anomaly detection for smart home based on user behavior. In: 2019 IEEE international conference on consumer electronics. ICCE, IEEE; 2019, p. 1–6.
[14] Ur B, McManus E, Pak Yong Ho M, Littman ML. Practical trigger-action programming in the smart home. In: Proceedings of the SIGCHI conference on human factors in computing systems. 2014, p. 803–12.
[15] Bitdefender. The 2024 IoT security landscape report. 2024, https://rb.gy/7h95ho.
[16] Boeckl K, Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas KN, Nadeau E, O'Rourke DG, Piccarreta B, Scarfone K. Considerations for managing internet of things (IoT) cybersecurity and privacy risks. US Department of Commerce, National Institute of Standards and Technology; 2019.
[17] Bugeja J, Jacobsson A, Davidsson P. On privacy and security challenges in smart connected homes. In: 2016 European intelligence and security informatics conference. EISIC, IEEE; 2016, p. 172–5.
[18] Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. Computer 2017;50(7):80–4.
[19] MITRE. MITRE ATT & CK, https://attack.mitre.org/.
[20] MITRE. CAPEC, https://capec.mitre.org/index.html.
[21] NIST. Tactics, Techniques, and Procedures (TTPs), https://rb.gy/2umu8q.
[22] Martin L. The Cyber Kill Chain, https://lmt.co/46AXLdz.
[23] Abiodun OI, Abiodun EO, Alawida M, Alkhawaldeh RS, Arshad H. A review on the security of the internet of things: Challenges and solutions. Wirel Pers Commun 2021;119:2603–37.
[24] Bipartisan Policy Center. Smart homes and policy: Cybersecurity risks and tradeoffs. 2022, https://rb.gy/f43z37.
[25] Wendzel S. How to increase the security of smart buildings? Commun ACM 2016;59(5):47–9.
[26] Guhr N, Werth O, Blacha PPH, Breitner MH. Privacy concerns in the smart home context. SN Appl Sci 2020;2:1–12.
[27] Hall F, Maglaras L, Aivaliotis T, Xagoraris L, Kantzavelou I. Smart homes: Security challenges and privacy concerns. 2020, arXiv preprint arXiv:2010.15394.
[28] Kuyucu MK, Bahtiyar Ş, İnce G. Security and privacy in the smart home: A survey of issues and mitigation strategies. In: 2019 4th international conference on computer science and engineering. UBMK, IEEE; 2019, p. 113–8.
[29] Zimmermann V, Gerber P, Marky K, Böck L, Kirchbuchner F. Assessing users' privacy and security concerns of smart home technologies. I- Com 2019;18(3):197–216.
[30] Ansari AM, Nazir M, Mustafa K. Smart homes app vulnerabilities, threats, and solutions: A systematic literature review. J Netw Syst Manage 2024;32(2):29.
[31] IoT cybersecurity: strengthening defenses against threats. American Public University, https://rb.gy/t9xam0.
[32] Alshboul Y, Bsoul AAR, Al Zamil M, Samarah S. Cybersecurity of smart home systems: Sensor identity protection. J Netw Syst Manage 2021;29(3):22.
[33] Ali B, Awad AI. Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors 2018;18(3):817.
[34] Touqeer H, Zaman S, Amin R, Hussain M, Al-Turjman F, Bilal M. Smart home security: Challenges, issues and solutions at different IoT layers. J Supercomput 2021;77(12):14053–89.
[35] Rapid7. Metasploit, https://www.metasploit.com.
[36] Nmap ORG. Nmap, https://nmap.org.
[37] IoTAC. 8 attacks against a smart home every 24 h. 2023, https://rb.gy/acooq4.
[38] Micro T. Inside the smart home: IoT device threats and attack scenarios. 2019, https://rb.gy/1z6x5q.
[39] Andrade RO, Ortiz-Garcés I, Cazares M. Cybersecurity attacks on smart home during Covid-19 pandemic. In: 2020 fourth world conference on smart trends in systems, security and sustainability (worldS4). IEEE; 2020, p. 398–404.
[40] Apthorpe N, Reisman D, Sundaresan S, Narayanan A, Feamster N. Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic. 2017, arXiv preprint arXiv:1708.05044.
[41] Alberts C, Dorofee A, Stevens J, Woody C. Introduction to the OCTAVE approach. Pittsburgh, PA: Carnegie Mellon University; 2003, p. 72–4.
[42] MITRE. Common weakness enumeration. 2024, https://cwe.mitre.org/.
[43] Heartfield R, Loukas G, Budimir S, Bezemskij A, Fontaine JR, Filippoupolitis A, Roesch E. A taxonomy of cyber-physical threats and impact in the smart home. Comput Secur 2018;78:398–428.
[44] Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M. Cybersecurity challenges in the maritime sector. Network 2022;2(1):123–38.
[45] Schinas O, Metzger D. Cyber-seaworthiness: A critical review of the literature. Mar Policy 2023;151:105592.
[46] Bugeja J, Jacobsson A, Davidsson P. PRASH: A framework for privacy risk analysis of smart homes. Sensors 2021;21(19):6399.
[47] Flores M, Heredia D, Andrade R, Ibrahim M. Smart home IoT network risk assessment using Bayesian networks. Entropy 2022;24(5):668.
[48] Pturgess J, Nurse JR, Zhao J. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In: Living in the internet of things: cybersecurity of the ioT-2018. IET; 2018, p. 1–8.
[49] Wang Y, Zhang R, Zhang X, Zhang Y. Privacy risk assessment of smart home system based on a STPA–FMEA method. Sensors 2023;23(10):4664.
[50] Park M, Oh H, Lee K. Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. Sensors 2019;19(9):2148.
[51] Arat F, Akleylek S. A new method for vulnerability and risk assessment of IoT. Comput Netw 2023;237:110046.

[52] Collen A, Nijdam NA. Can I sleep safely in my smarthome? A novel framework on automating dynamic risk assessment in IoT environments. Electronics 2022;11(7):1123.
[53] Alalade ED, Mahyoub M, Matrawy A. Privacy engineering in smart home (SH) systems: A comprehensive privacy threat analysis and risk management approach. 2024, arXiv preprint arXiv:2401.09519.
[54] Parsons EK, Panaousis E, Loukas G. How secure is home: Assessing human susceptibility to IoT threats. In: Proceedings of the 24th pan-hellenic conference on informatics. 2020, p. 64–71.
[55] Pandey P, Collen A, Nijdam N, Anagnostopoulos M, Katsikas S, Konstantas D. Towards automated threat-based risk assessment for cyber security in smarthomes. In: Proceedings of the 18th European conference on cyber warfare and security (ECCWS 2019), Coimbra, Portugal. 2019, p. 4–5.
[56] Wongvises C, Khurat A, Fall D, Kashihara S. Fault tree analysis-based risk quantification of smart homes. In: 2017 2nd international conference on information technology. INCIT, IEEE; 2017, p. 1–6.
[57] Jacobsson A, Boldt M, Carlsson B. A risk analysis of a smart home automation system. Future Gener Comput Syst 2016;56:719–33.