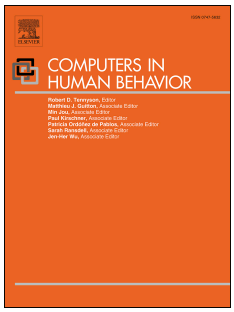

The digital harms of smart home devices: A systematic literature review

David Buil-Gil, Steven Kemp, Stefanie Kuenzel, Lynne Coventry, Sameh Zakhary, Daniel Tilley, James Nicholson

PII: S0747-5632(23)00121-8

DOI: https://doi.org/10.1016/j.chb.2023.107770

Reference: CHB 107770

To appear in: *Computers in Human Behavior*

Received Date: 30 August 2022

Revised Date: 18 February 2023

Accepted Date: 27 March 2023

Please cite this article as: Buil-Gil D., Kemp S., Kuenzel S., Coventry L., Zakhary S., Tilley D. & Nicholson J., The digital harms of smart home devices: A systematic literature review, *Computers in Human Behavior* (2023), doi: https://doi.org/10.1016/j.chb.2023.107770.

David Buil-Gil: Conceptualization; Methodology; Software; Formal analysis; Writing - Original Draft

Steven Kemp: Methodology; Formal analysis; Writing - Original Draft

Stefanie Kuenzel: Conceptualization; Methodology; Validation; Writing - Review & Editing

Lynne Coventry: Conceptualization; Methodology; Validation; Writing - Review & Editing

Sameh Zakhary: Conceptualization; Methodology; Validation; Writing - Review & Editing

Daniel Tilley: Conceptualization; Methodology; Validation; Writing - Review & Editing

James Nicholson: Conceptualization; Methodology; Validation; Writing - Review & Editing; Project administration

The digital harms of smart home devices: A systematic literature review

David Buil-Gil[1], Steven Kemp[2], Stefanie Kuenzel[3], Lynne Coventry[4], Sameh Zakhary[5], Daniel Tilley[6] and James Nicholson[7]

[1]Department of Criminology, University of Manchester, UK
[2]Department of Law, Pompeu Fabra University, Spain
[3]Department of Electronic Engineering, Royal Holloway University of London, UK
[4]Division of Cybersecurity, Abertay University, UK
[5]Zakhary IT Services Limited, UK
[6]Daniel Tilley Analytic Solutions Limited, UK
[7]Department of Computer and Information Sciences, Northumbria University, UK

Corresponding author

David Buil-Gil, 4.44 Williamson Building, Department of Criminology, University of Manchester, Oxford Road, Manchester M13 9PL, UK. Email: david.builgil@manchester.ac.uk

Acknowledgment

This work is funded by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity.

1. Introduction

The connection of electronic devices to the internet allows remote control of physical devices and involves remote collection and sharing of large volumes of data. "Internet-of-Things" (IoT) is the term used to refer to physical objects embedded with sensors and software that connect them to other devices and systems over the internet (Atzori et al., 2010; Weber, 2010). Since the early 1980s, when a group of researchers from Carnegie Mellon University connected a Coca-Cola vending machine to the internet for the first time, the IoT paradigm has expanded to encompass many different types of physical devices, including corporate security systems, connected cars, electrical grids, military equipment, and home appliances. The connection of home electronic devices and attributes to the internet is known as "smart home" (Lutolf, 1992). Smart homes may incorporate remote-controlled lighting, heating and water consumption, smart meters and internet-connected home security systems, as well as other home devices such as televisions, door locks, remote baby or pet control systems, refrigerators, or voice control devices (e.g., Google Home, Amazon Alexa). Almost any home electrical appliance can be connected to the internet, and multiple interconnected devices form smart home ecosystems. Smart home technologies are used not only to activate and deactivate appliances, but also to monitor the activities of households and automate certain aspects of everyday life (Ricquebourg et al., 2006). The use of IoT home devices is increasingly widespread: in the UK, a survey conducted by techUK and GfK in 2021 showed that 58% of respondents owned a smart TV, 39% smart speakers, 24% smart fitness and activity trackers and 15% smart thermostats (techUK, 2021). In March 2022, 51% of all meter readers in the UK were smart or advanced meters (BEIS, 2022).

While smart homes present many opportunities for users and may improve energy efficiency (Corbett, 2013), they also pose challenges to the security and privacy of users (Ali et al., 2017; Komninos et al., 2014). With the increase in the uptake of IoT home devices, it becomes critical to understand the digital harms that can be associated with smart homes. The main challenge of smart homes is related to the large amount of security-critical and privacy-sensitive data they record from users (Dorri et al., 2017). Lin and Bergmann (2016) argue that smart homes may pose threats to *confidentiality* (i.e., unwanted release of sensitive information), *authentication* (i.e., control or sensing information being falsified) and *access* (i.e., unauthorised access to system controls). For instance, *confidentiality* breaches may lead to an unwanted release of information about electricity usage that may inform potential offenders about the times when a house is not occupied (Blythe and Johnson, 2021; Hodges, 2021). *Confidentiality* breaches may also lead to a loss of sensitive medical data or other types of sensitive information, that can be used by offenders to hold data to ransom (Tzezana, 2016). An *authentication* threat may exist, for example, if an automated fire control system is tampered with to activate the emergency alarm system and unlock all doors, thus enabling anyone to access the building (Jacobsson et al., 2016). Unauthorised *access* to smart home control systems may enable the activation of webcams and voice control devices, or control of home appliances such as ovens or electric stoves, thus making the entire smart home ecosystem insecure. Smart homes may also enable new forms of cyberstalking and exacerbate power asymmetries between household members (Nicholls et al., 2020).

For all these reasons, it becomes crucial to fully understand the digital harms of smart homes, in terms of threats to privacy and security. A growing body of research has begun to speculate about the security and privacy challenges of IoT home devices, and record data about digital harms known to public authorities and users' perceptions and experiences. The field is now at a point where these unique studies can be synthesised to create a comprehensive review of the digital harms of smart homes, which may serve to further inform policy and sociotechnical solutions to mitigate them. This article presents a systematic review of the literature using observational, experimental, documental, or case study research methods to analyse the security and privacy harms of smart home applications and technologies. Previously, Marikyan et al. (2019) conducted a systematic review of studies published between 2002 and 2017 to explore the definitions, services and functions of smart homes and the main motivations for smart home adoption. They highlighted that one of the main barriers to the adoption of smart devices was the high perceptions of privacy and security risks among users. Blythe and Johnson (2021) conducted a systematic review of articles published between 2007 and 2017 to analyse crimes facilitated by consumer IoT. Other systematic reviews have also synthesised the literature about the security challenges of smart cities (Laufs et al., 2020) and applications of smart homes to monitor the well-being of older adults (Demiris and Hensel, 2008). Our research builds on and expands previous literature reviews about the privacy and security harms of smart homes. More specifically, the aims and expected contribution of this article are:

- Classify the digital harms of smart homes;
- Identify smart home devices and attributes that pose digital harms; and
- Explore policy and sociotechnical approaches to mitigate the digital harms of smart homes.

To our knowledge, this is the first systematic review of the literature to specifically focus on the digital harms of smart homes. Importantly, the use of smart home appliances has increased rapidly since the last systematic review of crimes facilitated by consumer IoT, which was conducted in 2017 (Blythe and Johnson, 2021), and many new digital harms may have emerged since then. For instance, according to estimates by techUK (2021), the ownership of smart speakers increased by 81% between 2017 and 2021, and this increase was larger than 75% in the case of smart doorbells, 50% in smart lighting, 49% in smart TVs and 47% in smart thermostats. Gaining a better understanding of the digital harms of smart homes is essential to design technical, social and socio-technical mechanisms to protect the data and prevent the harms specific to each device, user and context.

Moreover, synthesising existing evidence on the digital harms of smart devices is essential to further contribute to the development of theoretical frameworks aimed at explaining the adoption and implementation of IoT technologies. The theoretical and conceptual model developed by Nord et al. (2019), for instance, argues that the adoption and implementation of IoT devices is dependent upon the links between the priorities of stakeholders, the networks of devices and applications, the privacy and security challenges of devices, and people's trust in IoT. Our systematic review presents key information to better understand the privacy, security and trust challenges of IoT devices in home settings, thus contributing to the growing theoretical base on IoT adoption and implementation.

This article is structured as follows: Section 2 presents an overarching description of recent developments in smart home ecosystems. Section 3 describes the methodology of the systematic

review, including the search strategy, selection of studies, and data extraction. Section 4 presents the results, and Section 5 presents the discussion and final conclusions.

2. Smart home: Opportunities and digital harms

Marikyan et al. (2019) identified four broad areas in which smart home devices can provide benefits for users: health-related benefits (e.g., detection of dangerous events), environmental benefits (e.g., reduction in electricity consumption), financial benefits (e.g., cheaper virtual visits), and psychological wellbeing and social inclusion (e.g., virtual interaction and entertainment). These benefits coincide with the most relevant benefits found by Sovacool and Furszyfer Del Rio (2021) in their study using expert interviews, though these authors also highlight the relevance of "convenience and controllability" provided by smart homes (see also Lee et al., 2017). However, in addition to the potential benefits, it is also key to understand the risks and barriers of smart home technologies.

There are multiple ways consumer IoT can be exploited for crime (Blythe and Johnson, 2021), and it is easy to find examples of attacks involving smart home devices. Possibly the most famous of these is the Mirai botnet, which exploits poor security in IoT devices and has been used in numerous disruptive Distributed Denial-of-Service (DDoS) attacks around the world (Krebs, 2017). The authors of the initial attacks in 2016 published the source code for Mirai, meaning it was reused and sold as a DDoS-for-hire service. In 2017, the developers of the Mirai malware were also found guilty of infecting IoT devices and home routers to create another botnet that was used in a click-fraud scam to generate illicit advertising revenue (US Department of Justice, 2017). Other well-known attacks have involved the hacking of home cameras that are used for security and baby monitoring, thereby allowing private videos to be freely viewed online (BBC, 2013). Relatedly, research has highlighted the role of smart home devices in domestic abuse (Nicholls et al., 2020).

Outlining just a few examples of attacks that have used smart home devices provides an insight into the wide range of potential harms from these technologies. This has not gone unnoticed by government agencies. For instance, in the UK, the Product Security and Telecommunications Infrastructure (PSTI) Bill was recently processed by the legislator, with the department behind the bill stating that its objective is to protect against "the harms enabled through insecure consumer connectable products" (DCMS, 2021a). This legislation links closely to the concept of safety by design that was explicitly noted in the UK Government Online Harms White Paper from 2019 (DCMS, 2019) and to the definition of "online harms" in the government's draft Online Safety Bill: "user generated content or behaviour that is illegal or could cause significant physical or psychological harm to a person" (DCMS, 2021b).

However, this official definition may not cover the first two examples of botnet-based attacks described above, since these do not necessarily cause physical or psychological harm to a person. Thus, to fully understand the digital harms related to smart home devices a more tailored definition and classification is necessary. Unfortunately, despite the clear policy interest in harms from smart home devices (Piasecki et al., 2021), an agreed-upon taxonomy does not exist. This is problematic because to prevent digital harms we first need to understand how these might arise. Establishing and prioritising policy responses necessitate a comprehensive assessment of potential harms (Agrafiotis et al., 2018).

To this end, we have adapted classifications of online harms by McGuire and Dowling (2013), Wall (2001), and Lin and Bergmann (2016) in accordance with the nature, objective, and method of online harm, respectively (Table 1). Firstly, with regard to the nature of harm, this is divided into cyber-dependent harms that can only occur online, such as DDoS attacks, and cyber-enabled harms that can also take place offline but are increased in scope by the internet, for example, fraud or stalking. In the second place, the objective of the harm is more akin to a legal categorisation. It includes (a) 'cyber-trespass' when invisible boundaries are crossed, such as hacking a computer system, (b) 'cyber-deception and theft', for example, the myriad of possible frauds committed over the internet, (c) 'cyber-porn and obscenity', which can sometimes not necessarily be illegal, and (d) 'cyber-violence', which involve injurious or hurtful behaviour such as stalking. Finally, we adapt a classification of the method used to bring about the harm (Lin and Bergmann, 2016). This can be achieved by the unwanted release of information (confidentiality), falsification of control or sensing information (authentication), or unauthorised access to system controls (access). We will apply this classification to record information about digital harms from articles included in the systematic literature review.

Table 1. Proposed classifications of online harms

Classification	Definition	Examples
According to nature of harm. Adaptation of classification by McGuire and Dowling (2013)		
Cyber-dependent harm	Harms that can only be committed through the internet and do not have an equivalent offline mode	Malware, DoS, hacking
Cyber-enabled harm	Harms that have an offline equivalent mode but have increased in reach and impact due to the internet	Fraud, stalking, grooming
According to objective of harm. Adaptation of classification by Wall (2001)		
Cyber-trespass	Crossing of invisible boundaries of ownership online	Hacking, access to private/confidential data
Cyber-deception and theft	Harmful or criminal acquisitions that occur online	Fraud, identity theft, digital piracy
Cyber-porn and obscenity	Deviant content related with sex and pornography	Pornography, sexual services, online child sexual exploitation
Cyber-violence	Injurious, hurtful or dangerous materials	Stalking, harassment, terrorism
According to method of harm. Adaptation of classification by Lin and Bergmann (2016)		
Confidentiality	Unwanted release of sensitive information	Release of information about electricity usage, explicit photos
Authentication	Control or sensing information being falsified	False data injection, system tempered with to unlock doors
Access	Unauthorised access to system controls	Activation of web cam, control of voice assisted device

3. Methodology

This article takes a two-fold methodological approach to synthesising the recent literature about the digital harms related to smart homes. First, we systematically review all relevant studies published between January 2011 and October 2021. By systematically reviewing the literature we aimed to classify the digital harms related to smart homes, identify the smart home devices and attributes that pose digital harms, and explore potential policy and sociotechnical approaches to mitigate digital harms. We have restricted our search to studies published since 2011 due to the rapid technological development of smart technologies and to facilitate the search. Second, where possible, we illustrate the findings of the literature review with real-world cases.

We conduct the systematic literature review using a-priori criteria to search, select and extract data from studies. The systematic review protocol follows the Preferred Reporting Items for Systematic reviews and Meta-Analyses for Protocols 2015 (PRISMA), which is a widely used checklist to facilitate the design of robust protocols for systematic reviews (Mohler et al., 2015). The following sections explain the systematic review protocol in detail.

3.1 Search strategy

We have selected articles that use observational, experimental, documental, or case study research methods to analyse the security and privacy harms of smart homes. Thus, we do not include theoretical or technical notes or reviews of the literature. We have included peer-reviewed studies published in English. Since this article is particularly interested in smart homes, we have excluded all studies that analyse related technologies in settings that are not solely residential (e.g., IoT for cities, business, healthcare or any other context). We have also excluded those studies that explore smart homes but do not consider their digital harms, either privacy- or security-related.

The search for published studies was conducted in October 2021. The following databases were used to search for published articles: Web of Science and Scopus. Both databases provide access to multiple multidisciplinary and regional citation indices. Web of Science covers more than 182 million records in engineering, social sciences, natural sciences, biomedical sciences and arts and humanities, with its strongest coverage in engineering, computer science and natural sciences. It covers several databases such as the Web of Science Core Collections, BIOSIS, SciELO and Data Citation Index. Scopus includes more than 77 million items from more than 5,000 publishers in many different fields, including computing, information sciences, law, human society and engineering. Major publishers included in the Web of Science database include Springer, Nature, Wiley, IEEE, Elsevier and ACM. Thus, Web of Science and Scopus include many other digital libraries, such as IEEE Xplore and ACM Digital Library.

The search strategy used the following search terms in titles, abstracts, keywords and subject headings:

> (((SMART) OR (IOT) OR (INTERNET OF THINGS) OR (AUTOMAT) OR (VIRTUAL)) AND ((HOME) OR (HOUSE) OR (DOMESTIC) OR (RESIDEN)) OR (DOMOTICS)) AND ((SECUR) OR (PRIVA) OR (CRIM) OR (HACK) OR (ATTACK) OR (INCIDENT) OR (BREACH) OR (LEAK) OR (HARM) OR (THEFT))

Some terms were truncated to include all related terms. For example, "AUTOMAT" includes automation, automated and automating, "HACK" includes hack, hacking and hacker, and "SECUR" includes "secure", "security" and "cybersecurity". The search strategy was agreed among all co-authors after consulting several practitioners working in public and private sector organisations.

3.2 Selection of studies

All 3,147 identified citations were imported into a database. Duplicated citations were removed. Two researchers then screened the titles and abstracts of all articles against our inclusion criteria, namely: (a) main focus is on smart home appliances or attributes, (b) explores privacy and/or security harms, (c) uses data recorded from observation, case studies, documents or experiments, either quantitative or qualitative, and (d) is available in English. In order to ensure consistency among data collectors, we then selected random samples of 100 citations and shared them with five additional researchers, who also screened the titles and abstracts against our inclusion criteria. Interrater reliability scores were then calculated, showing moderate-strong levels of agreement for criteria (a) (% agreement = 84.4, Cohen's κ = 0. 67, p-value < 0.001) and (b) (% agreement = 83.8, Cohen's κ = 0. 68, p-value < 0.001), and moderate levels of agreement for criteria (c) (% agreement = 80.0, Cohen's κ = 0. 50, p-value < 0.001) and (d) (% agreement = 97.0, Cohen's κ = 0. 53, p-value < 0.001). The interrater reliability was moderate-strong for the overall inclusion of studies (% agreement = 89.0, Cohen's κ = 0. 68, p-value < 0.001). Disagreements were resolved through consensus between the two primary judges, and all studies that did not meet one or more criteria were removed from our review.

The PRISMA flowchart in Figure 1 shows the process of selection of studies. The main reason for excluding articles was that the primary focus of the study was not on smart homes. In total, 1,977 studies did not meet this criterion, amongst which many of them were studies with a focus on smart cities, smart farms or smart automobiles. 1,402 studies were not selected for failing to meet the criterion of studying harms. Many of those, for instance, focused on the energy efficiency, regulatory requirements, military applications or security perceptions related to IoT devices in home settings or elsewhere. 533 studies did not use data obtained from observational, case, documental or experimental studies (e.g., literature reviews, technical reviews, theoretical pieces). We also excluded 111 studies that either were not available in English or not available at all.

While interrater reliability indices show a moderate-strong degree of inter-judge reliability, the volume of selected studies was still too large for an exhaustive review of studies (k = 625). We thus considered a fifth inclusion criterion that reduced the number of selected studies: (e) analyses of real-world harms on real-world smart home appliances or attributes, thus excluding both laboratory experiments that do not attack real-world devices and computer simulations not based on real-world data. 588 studies were removed for this reason. Finally, 67 studies met the inclusion criteria and were subject to an in-depth review. After reviewing the content of selected articles, 4 studies were excluded from the analysis due to failing to meet at least one of our main selection criteria (i.e., 2 did not study digital harms, and 2 did not analyse data obtained from observational, case, documental or experimental studies). 63 studies were included in the literature review. A short description of each study is included in Table 2, including a unique identification number for each study, which will be used to refer to it in text.

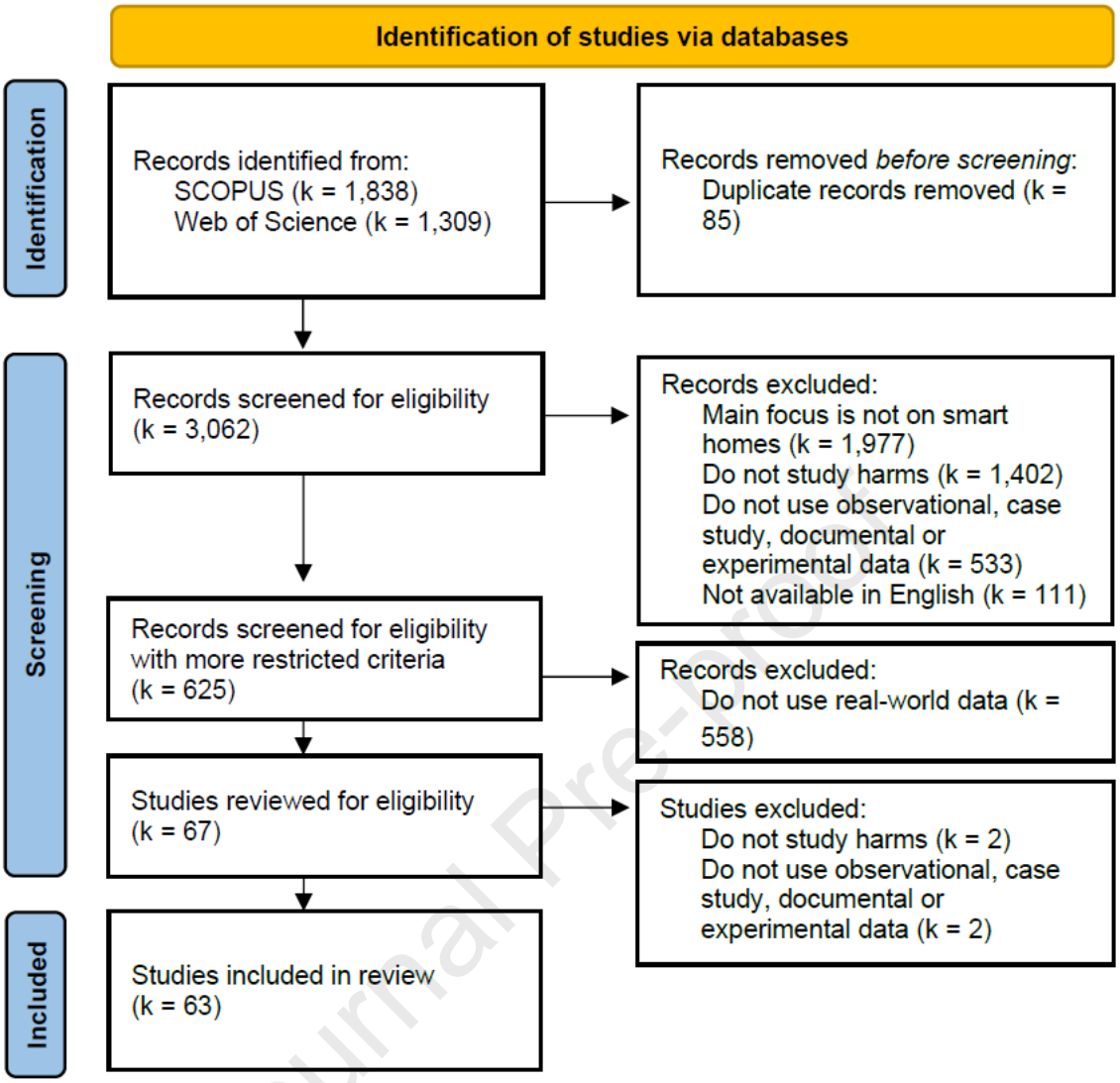

Figure 1. PRISMA flowchart in the selection of studies

Table 2. Summary description of primary studies included in the systematic review

	Paper	Topic of study
1	Javed et al. (2021)	Spoofing countermeasures against voice assistants
2	Anthi et al. (2021)	Adversarial Machine Learning against Intrusion Detection Systems
3	OConnor et al. (2021)	Protecting companion apps against man-in-the-middle attacks
4	Yu et al. (2021)	Sensitive information in the metadata of encrypted packets
5	Tran et al. (2021)	Voice replay and injection attacks against voice assistants
6	Wang, Li et al. (2021)	Decision tree models to detect attacks against smart devices
7	Li et al. (2021)	Automation of privacy policy statements for smart home apps
8	Tushir et al. (2021)	Impact of DoS attacks on smart devices connected to WiFi
9	AlOtaibi and Lombardi (2021)	Sound- and network-based attacks against Amazon Echo
10	Yamauchi et al. (2021)	Machine learning to detect anomalous behaviour
11	Aafer et al. (2021)	Technical vulnerabilities of Android Smart TV
12	Wang, Ji et al. (2021)	Automation of security assessment of IoT messaging protocols
13	Wan et al. (2021)	Unveiling of smart devices from network data
14	Rauti et al. (2021)	Man-in-the-browser attacks to intercept/modify data
15	Heartfield et al. (2021)	Self-configurable automated intrusion detection system
16	Choi et al. (2021)	Older adults' experiences with smart devices
17	Cultice et al. (2020)	Machine learning to detect anomalous data
18	Alsheakh and Bhattacharjee (2020)	Automated quantification of security of smart devices
19	Gassais et al. (2020)	Self-configurable automated intrusion detection system
20	Peng and Wang (2020)	Network-based monitoring platform to identify security threats
21	Xiao et al. (2020)	Authentication framework to protect devices from attacks related to open ports and over-privilege
22	Salomons et al. (2020)	Hardware and control model to protect data in water meters
23	Wang et al. (2020)	Inferred voice commands against voice assistants
24	Sikder et al. (2020)	Access control system for multiple users and devices
25	Li et al. (2020)	Identification of user behaviour from traffic data of cameras
26	Zainab et al. (2020)	Machine learning to identify spam in smart devices
27	Bugeja et al. (2020)	Smart devices' software vulnerabilities to DoS attacks
28	Vidal-González et al. (2002)	Malware attacks against smart homes
29	Bistarelli et al. (2020)	Malware attacks against smart homes
30	Hariri et al. (2020)	Man-in-the-middle attack to exploit the heartbeat of devices
31	Skowron et al. (2020)	Machine Learning to identify devices and users' activities
32	Javed and Rajabi (2020)	AI-based solution for malicious traffic detection
33	Sikder et al. (2019)	Markov Chain Machine Learning to detect malicious activity
34	Leitão (2019)	Smart devices as attack vectors for intimate partner violence
35	Kennedy et al. (2019)	Voice command fingerprinting attacks against home speakers
36	Martin et al. (2019)	Malware against Raspberry Pi smart devices
37	Ullrich et al. (2019)	Vulnerabilities of the firmware of robot vacuum cleaners
38	Zhang et al. (2019)	Blockchain-based security protocol to protect IoT networks
39	Alkhatib et al. (2019)	Developers' insights into the privacy of elderly monitoring devices
40	Mahadewa et al. (2018)	Integrated perspective to identify vulnerabilities of smart homes
41	Zhang et al. (2018)	Identification of malicious smart home apps
42	Jia et al. (2018)	Graph-based mechanism to identify vulnerabilities of smart homes
43	Anthi et al. (2018)	Security of adaptive IoT hub for smart home ecosystems
44	Isawa et al. (2018)	Disassembly-code-based similarity between IoT malware
45	Bhatt and Morais (2018)	Anomaly detection system for smart homes
46	Do et al. (2018)	Adversarial models to identify vulnerabilities of smart devices
47	Bordel et al. (2018)	Large datasets reduction for smart home security systems
48	Sivanathan et al. (2018)	Penetration testing to assess the security of consumer IoT devices
49	Lally and Sgandurra (2018)	Framework to evaluate vulnerabilities of smart devices
50	Ji et al. (2018)	Eavesdropping of smart wireless cameras
51	Mashima et al. (2018)	Estimation of sensitive information from energy usage data
52	Teng et al. (2017)	Over-the-air firmware update system for routers and gateways

53	Fan et al. (2017)	Obfuscation of reactive power demand of smart meters
54	Lyu et al. (2017)	Capacity of consumer IoT devices to participate in DDoS attacks
55	Sivanathan et al. (2017)	Flow-based network monitoring to identify attacks
56	Han and Park (2017)	Push button configuration to detect unintended paired devices
57	Capellupo et al. (2017)	Identification of security vulnerabilities of smart devices
58	Birchley et al. (2017)	Ethical issues of smart health devices
59	Copos et al. (2016)	Network traffic analysis to infer sensitive household information
60	Min and Varadharajan (2016)	Feature-distributed malware to compromise internet services of IoT
61	de Morais et al. (2014)	Active in-database processing to protect data of ambient-assisted living (AAL)
62	Matern et al. (2013)	Detection of events in AAL using sensor data
63	Boise et al. (2013)	Older adults' experiences with unobtrusive home monitoring

3.3 Data extraction

Two researchers then reviewed all selected articles and extracted data from them using a standardised form. Aside from information about the year of publication, type of publication, authors, and name of the journal or conference proceedings, which was downloaded automatically from the databases, we recorded detailed information from each article and coded the data into the following categories: (a) design of the study, (b) main aims, (c) type of data analysed, (d) research field, (e) country of authors, (f) country and agency that provided funding, (g) country where data was recorded, (h) smart devices analysed, (i) digital harms identified (by harm type, and according to the categorisation presented in Table 1), (j) type of data that pose a threat or vulnerability, (k) policy or sociotechnical recommendation to mitigate harms, (l) focus of recommendation, and (m) other relevant findings.

For each of these variables, we coded articles according to predefined categories and free-text descriptions with detailed information. For example, to code the design of the study, we distinguished between descriptive, correlational, experimental, meta-analysis, and other types of studies, and then coded all details about the design of each research. Similarly, to study the focus of the recommendation, we distinguished between studies that propose harm prevention or reduction measures focused on the perpetrator, target (e.g., smart device, data), user, or guardian (e.g., third parties that can protect the target or user, such as manufacturers that monitor emerging harms, family members) (Leukfeldt and Yar, 2016), as well as details about the specific recommendation proposed. We also counted the number of citations of each article according to Google Scholar on 20 April 2022. We will present descriptive statistics and tables for each variable.

3.4 Exemplar cases

In order to further illustrate some of the main findings from the systematic literature review, we accessed detailed information from real-world recorded cases and will present anonymised descriptions. More specifically, we obtained details from real cases reported to different police forces in the UK, organisational data breaches sentenced in court in the US and recorded in the Privacy Rights Clearinghouse (PRC) website (https://privacyrights.org/data-breaches), anonymised online reports to websites such as BitcoinAbuse (https://www.bitcoinabuse.com/), and media reports. We purposively and non-randomly select cases to illustrate common themes that arise from the systematic literature review. All accounts of real cases will be anonymised and described in general terms to preserve confidentiality.

4. Results

In Section 4.1 we present details about selected studies, including the research field and country of authors, organisations that provide funding, design of the study, aims, and type of data analysed. In Section 4.2 we describe the main types of harms identified and classify them. Finally, in Section 4.3 we summarise the approaches recommended to mitigate the digital harms of smart devices.

4.1 Description of selected studies

Amongst the 63 selected studies, 21 (33.3%) of them were published in journals and 42 (66.7%) in conference proceedings. The main journals were IEEE Access (3), Computers and Security (2), IEEE Internet of Things Journal (2) and Sensors (2); while only two conference proceedings were represented more than once (i.e., 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, and 30th USENIX Security Symposium). IEEE was the most frequent publisher both for journal articles and conference proceedings (7 and 22, respectively), followed by Elsevier (4) and MDPI (3) for journal articles, and Springer (8) and ACM (7) for conference proceedings.

As shown in Figure 2, there is an increase in the frequency of selected studies over time, with 2021 and 2020 being the years with the largest number of articles (16). We note however that data was recorded in October 2021, which in turn means 2021 was the year with the largest ratio of articles per month.

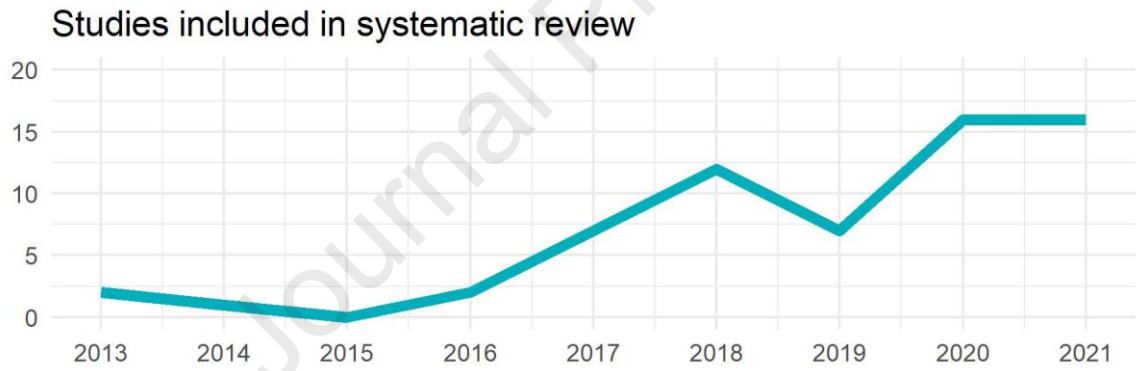

Figure 2. Studies included in systematic review by year of publication

While selected studies included researchers from across 23 countries[1], three countries were represented in the majority of studies: USA (25, 39.7%), China (12, 19.0%) and UK (9, 14.3%), as shown in Figure 3(a). 13 studies involved authors from across multiple countries. Similarly, as shown in Figure 3(b), amongst those studies that acknowledge a source of funding (43 out of 63), the main countries (or group of countries) that provide funding for research are USA (17, 39.5%), China (11, 25.6%), European Union (4, 9.3%) and UK (3, 7.0%). The most frequently mentioned funding entities were the USA National Science Foundation (10, 23.3%), Chinese National Natural Science Foundation (5, 11.6%), Chinese National Key Research and Development Program (4, 9.3%), and UK Engineering and Physical Sciences Research Council (3, 7.0%). 24 studies mentioned more than one funding

[1] Studies in the sample included researchers from Australia, Brazil, Canada, China, Finland, Germany, Israel, Italy, Japan, Kazakhstan, Norway, Pakistan, Poland, Portugal, Qatar, Saudi Arabia, South Korea, Singapore, Spain, Sweden, Taiwan, UK and USA.

source, and 7 of them obtained funding from more than one country. Aside from national research councils, some studies also acknowledged receiving internal funding from universities, and in some cases from private organisations such as Ericsson, Intel and Schneider. We also recorded information about the places where data were originally recorded, noticing that most of them recorded data in USA (21), UK (9), China (7) and Australia (5). One study analysed data recorded in 5 different countries [28].

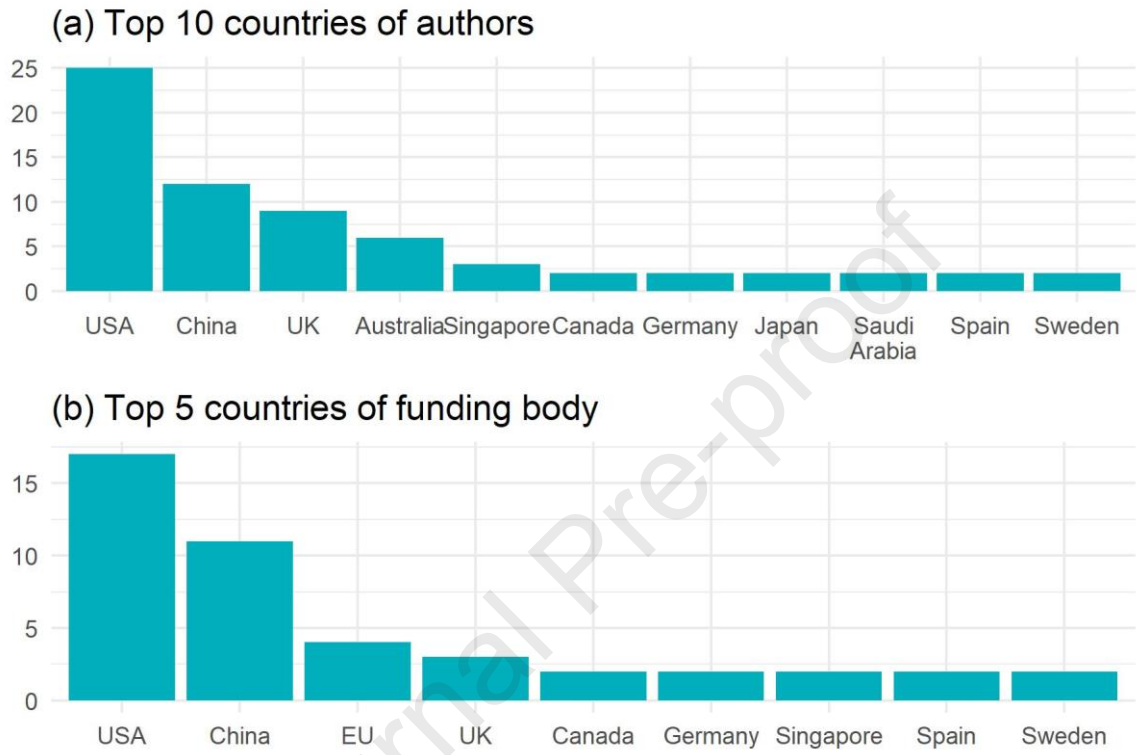

Figure 3. Main countries of authors and funding bodies of studies included in systematic review

Regarding the research fields of the authors (compiled from affiliations to university departments and research centres, and authors' bios included in publications), as shown in Figure 4, most authors were affiliated to computer science (39, 61.9%) or computer engineering (28, 44.4%) departments or centres, and fewer to electrical engineering (15, 23.8%). Only 4 studies involved researchers from health disciplines and 1 from social sciences and humanities. We also noted an overall lack of interdisciplinary work, with very few studies involving researchers from different technical disciplines, and not a single study involving researchers from both technical and health or social sciences.

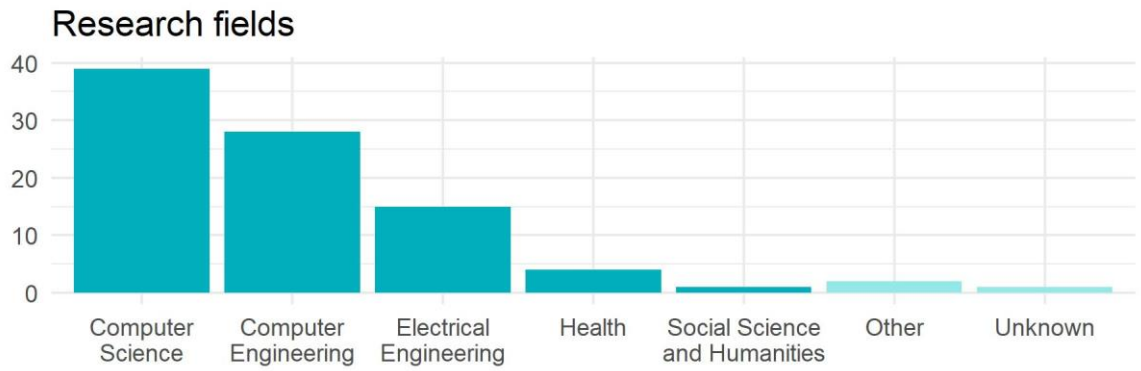

Figure 4. Research field of researchers included in systematic review

The majority of studies (52, 82.5%) were described as experimental or quasi-experimental by design (i.e., introducing a change, such as exploiting a vulnerability or applying software updates, to experimental groups, such as smart devices or smart home ecosystems, to identify effects in the outcome variables). For instance, [1] tests a spoofing countermeasure for voice assistant systems (e.g., Google Home, Amazon Alexa) against a set of voice spoofing attacks, including synthetic voice attacks and cloned replay attacks; [33] evaluates the effectiveness of a context-aware security framework based on Markov processes to detect malicious actions in smart homes; [48] rates the security level of IoT devices through penetration testing tools; and [50] eavesdrops wireless smart camera traffic to identify the presence of people in the house. Fewer studies were identified as descriptive by design (22, 35.0%). Some examples include [28], [29] and [36], which used honeypots to capture active malware targeting smart homes, thus allowing researchers to examine the characteristics of identified malware; and [39], which used semi-structured interviews with developers to gain a better understanding of privacy issues of aged care monitoring devices. 11 studies combined descriptive and experimental designs. No study followed correlational or meta-analytical designs. The information about the methodological design of studies was recorded from their methods' descriptions, regardless of the overall quality of the design of the study (e.g., sample sizes, randomisation processes, significance tests). We return to this point in the Discussion section.

The majority of studies recorded primary quantitative data (52, 82.5%), such as the volume and characteristics of metadata of encrypted packets sent from smart devices [4], data sent from smart devices to web browser extensions [14], sensor device events [33], or surveys to older adults [63]. Primary qualitative data, including open code of smart apps [7], interviews with engineering researchers [58], and interviews and workshops with survivors of intimate partner violence and support workers [34], was recorded in 15 studies (23.8%). Finally, 8 studies analysed secondary quantitative data, including existing datasets of voice spoofing attacks [1] and real-world cyber-attacks and traffic data [18]. [34] analysed secondary qualitative data from discussions in domestic abuse forums. 11 studies analysed both quantitative and qualitative data.

Regarding the aims of studies, most of them aimed to study the vulnerabilities of specific smart home devices (34, 54.0%), followed by designing and/or evaluating technology solutions to reduce the digital harms of smart homes (33, 52.4%), and studying vulnerabilities of smart home ecosystems beyond specific devices (27, 42.9%). 27 studies aimed to identify vulnerabilities of smart homes and develop technology solutions. As an example, [20] designed and evaluated a network-based

monitoring platform to identify security threats against smart devices, and [23] executed attacks against smart speakers to infer voice commands and then proposed a differential privacy approach to protect such data.

We also recorded data about the number of citations of studies, showing a mean of 18.44 (min = 0, max = 122, median = 8). [41] was the study with the largest number of citations, 122, followed by [59] (114 citations) and [63] (112 citations).

4.2 Classifying the digital harms of smart homes

Firstly, we classified the digital harms identified in each study according to the type of incident, including cybercrimes listed by the UK Crime Prosecution Service (n.d.) (e.g., hacking, malware, DoS, stalking) and privacy intrusions more generally. As shown in Figure 5, privacy intrusions were the most common type of harm identified (31, 72.1%), followed by hacking (29, 67.4%), malware (22, 51.2%), DoS/DDoS (21, 48.8%) and stalking (3, 7.0%). Most studies identified different types of harms. Moreover, certain incidents can comprise different harms simultaneously. Examples of these types of harms, both obtained from the systematic literature review and our exemplar cases, are presented in Table 3.

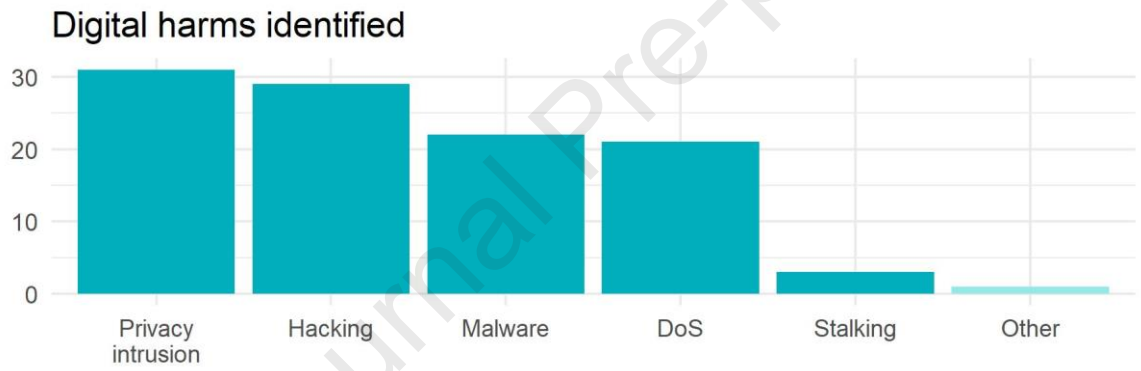

Figure 5. Digital harms (by type of incident) of smart homes

Table 3. Examples of digital harms identified in literature review and exemplar cases

	From literature review	From exemplar cases
Privacy intrusion	Breaches of smart water meters reveal home activities [22]	Smart doorbell camera invades neighbour's privacy (UK court case[2])
	Uncontrolled/unauthorised access to private data recorded by aged care monitoring devices [39]	App companion of smart sex toy records private moments without consent of the user (USA court case[3])
Hacking	Voice replay and voice injection attacks on voice assistants [5]	Smart TV hacked to access victim's personal details (UK police report)
	False data injection on smart devices [26]	Smart camera and baby monitor feeds from 700 households were hacked and published online (USA court case[4])
Malware	652,881 interactions with botnets targeting IoT devices [28]	Mirai malware disables CCTV, routers, and other devices (USA court case[5])
	8,713 IoT malware samples [44]	Botnet targeting smart home devices and requesting ransom (Bitcoinabuse report)
DoS/DDoS	Semantic DoS attacks on five smart home devices [27]	Devices infected with Mirai malware to carry our DDoS attacks (USA court case[6])
	DoS attacks on seven routers [52]	DDoS attacks on gaming networks (USA[7] and Finland[8] court cases)
Stalking	Controlling partner activities through smart cameras, thermostats, TVs and locks [34]	Control of ex-partner's activities through Amazon Alexa (UK police report)
	Inferring activity of household members from smart thermostat and air detector [59]	App companion of ELAN smart home system used to control ex-partner activities (UK police report)

One study identified a different type of harm that did not fall within the previous categories: traditional access control mechanisms in smart homes consider one unique type of trusted user (in binary terms: control or absence of control), which may lead to certain users being granted an undesired full access control to all devices in the smart home ecosystem [24]. In turn, the authors propose a platform to manage access rights for multiple devices and users.

Secondly, we classify the harms of smart homes according to the taxonomies presented by McGuire and Dowling (2013), Wall (2001), and Lin and Bergmann (2016), which had been previously explained in Section 2. Table 4 summarises the frequencies of studies that identified digital harms according to these three classifications. As before, most studies identified several types of harms and thus are counted in various categories. Based on McGuire and Dowling (2013), the majority of

[2] https://www.judiciary.uk/wp-content/uploads/2021/10/Fairhurst-v-Woodard-Judgment-1.pdf
[3] https://www.courthousenews.com/wp-content/uploads/2018/01/Lovense.pdf
[4] https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf
[5] https://www.justice.gov/usao-nj/press-release/file/1017616/download
[6] https://www.justice.gov/usao-nj/press-release/file/1017616/download
[7] https://www.justice.gov/usao-ndil/file/900826/download
[8] https://www.kaleva.fi/17-vuotias-tuomittiin-murtautumisesta-yli-50-000-p/1842675

studies identified cyber-dependent harms (58, 92.1%) – that is, incidents that can only take place online and do not have an equivalent offline mode. Only 8 studies identified cyber-enabled harms. Based on Wall (2001), 59 out of 63 studies (93.7%) focused on cyber-trespass (i.e., crossing online boundaries of ownership), while 9 studies identified harms related to cyber-deception (i.e., harmful acquisitions that occur online, such as identity theft or fraud). Only 3 studies identified cyber-violence and 2 cyber-porn/obscenity. Finally, according to the classification proposed by Lin and Bergmann (2016), 41 studies (65.1%) identified confidentiality, 41 (65.1%) access, and 24 (38.1%) authentication harms.

Table 4. Classification of digital harms identified in systematic review

		Trespass	Deception and theft	Porn and obscenity	Violence
Cyber-dependent	Confidentiality	34	5	1	2
	Authentication	23	6	1	2
	Access	38	8	1	2
Cyber-enabled	Confidentiality	7	0	1	2
	Authentication	3	1	0	1
	Access	4	1	0	1

As shown in Table 4, most studies focused on harms at the intersection of cyber-dependent, trespass, and access (38, 60.3%). For example, [21] identify harms related to the penetration of smart devices through exploiting open ports and over-privilege of companion apps, and [36] explore malware used to access Raspberry Pi IoT devices with weak credentials. 34 studies (54.0%) focused on harms at the intersection of cyber-dependent, trespass and confidentiality. For example, [59] applies network traffic analysis of data recorded by smart thermostats and air quality detectors to infer sensitive information about events occurring in a property, and [53] analyses reactive power data from smart meters to infer appliance usage information.

These types of harms have also been identified in our exemplar cases. For instance, in 2014, footage from 17 properties in the North East of England was hacked and live-streamed on a Russian website (UK police report), which aligns with the cyber-dependent, trespass, and confidentiality grouping. Similarly, in 2020 there was a Class Action Complaint against Ring LLC in the USA arguing that weak software security of smart cameras and doorbells allowed hackers to gain access to the control of these devices[9], which would be an example of cyber-dependent, trespass and access harm. An example of a cyber-dependent, trespass and authentication harm is identified in [26], which reports false data injections in smart home devices.

While these are the main types of harms identified in the systematic literature review, real-world examples of harms of smart devices exist for all groups in the taxonomy. For instance, a UK celebrity is currently facing trial for posting CCTV feeds of himself having sex with his ex-partner on various porn websites (UK police report), which would fall within a cyber-dependent, porn and confidentiality group. An example of a cyber-dependent and cyber-enabled, access and violence

[9] https://www.classaction.org/media/lemay-et-al-v-ring-llc.pdf

incident was seen in the hacking of Ring smart cameras and doorbells in 2020, which enabled perpetrators to threaten and racially abuse victims. And an example of cyber-enabled, violence and confidentiality harm can be found in a UK police report of someone who stalked his ex-partner through the app companion of an ELAN smart home system (UK police report).

4.3 Identifying smart home devices that may pose digital harms

We also recorded information about the types of devices associated with digital harms, and visualised results in Figure 6. The most referenced devices in our systematic review were security and surveillance systems (21, 33%), followed by lighting systems and smart bulbs (18, 28.6%) and voice control devices (15, 23.8%). For instance, [25] identifies user behaviour from traffic data of smart cameras, and [42] apply graph-based mechanisms to analyse traffic between Google Home smart speaker and TP-LINK light bulbs and identify vulnerabilities. Before we had seen several exemplar cases of harms related to security systems, such as the UK court case that concluded smart doorbell cameras invade neighbour's privacy, and the USA court case about home CCTV disabled by Mirai malware. Other types of devices that were less commonly referenced included temperature and ventilation devices (12, 19.0%), companion apps and browsers (12, 19.0%), and occupancy-aware control systems (10, 15.9%), amongst others.

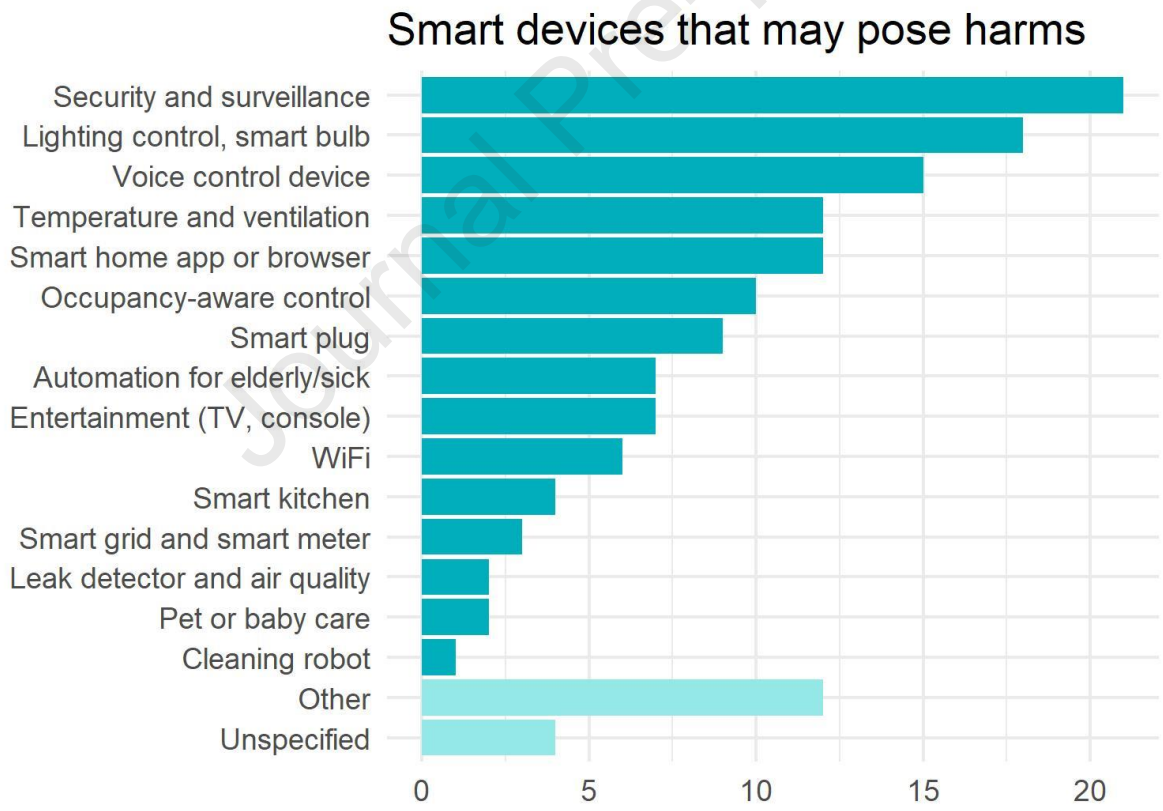

Figure 6. Smart devices that may pose harms identified in systematic review

It is important to bear in mind, however, that while the smart devices shown here may have been selected due to their actual digital harms or vulnerabilities, their selection may also be driven by the different uptake of devices in home settings, and even by researchers' preferences or the ease with which appliances can be studied. A report published by YouGov (2020) showed that the most

common type of smart device in UK households are smart meters (18% at the time of the study), followed by smart speakers (11%), thermostats (6%), lighting (5%) and security systems (3%). Another survey published by techUK (2021), which did not include smart meters, showed that 58% of respondents own smart TVs, 39% smart speakers, 24% smart fitness, 15% smart thermostats and 12% smart lighting. We thus find no direct correspondence between the most common types of devices identified in our review and the uptake of smart home devices, which shows that the usage of smart meters and smart TVs, for example, is more widespread than that of security and lighting systems. There is no data available to understand which types of devices are more commonly affected by digital harms in the real-world.

Further, we recorded data about the digital harms identified for different types of smart home devices (see Table 5) and the types of data that pose digital harms in each case (Table 6). The studies included in the systematic review identified that DoS/DDoS and privacy intrusions are more common in the case of security and surveillance systems, while hacking is more commonly identified for lighting systems and voice control devices. For instance, [30] disabled smart security systems through man-in-the-middle DoS attacks, [25] accessed private traffic data from cameras via WiFi sniffing, and [46] applied adversarial models to obtain information about household members and their routine activities from messages between smart lighting devices. DoS/DDoS attacks are also the most commonly identified type of harm in the case of WiFi and entertainment devices, while hacking is more common in the case of temperature and ventilation systems, smart home apps and browsers, smart plugs and smart kitchen appliances. Privacy intrusions are the most common type of harm for automation of elderly/sick and smart grids and meters.

Table 5. Digital harms identified for each smart home device

	Privacy intrusion	Hacking	Malware	DoS	Stalking
Security and surveillance	10	9	7	12	2
Lighting control, smart bulb	7	12	9	9	1
Voice control device	7	10	4	5	1
Temperature and ventilation	4	6	6	5	3
Smart home app or browser	4	7	6	3	1
Occupancy-aware control	4	6	6	5	1
Smart plug	5	8	5	4	1
Automation for elderly/sick	7	2	1	1	1
Entertainment	2	3	5	5	2
WiFi	2	4	1	5	0
Smart kitchen	0	4	3	1	0
Smart grid and smart meter	3	0	0	0	0
Leak detector and air quality	1	2	2	2	1
Pet or baby care	1	1	1	2	0
Cleaning robot	1	1	0	1	0

Regarding the type of data that may pose vulnerabilities, network traffic data was the most mentioned in our selection of studies (24, 38.1%), followed by energy usage data (13, 20.6%), written communications (10, 15.9%), audio (9, 14.3%), image (7, 11.1%) and video (7, 11.1%). These, nonetheless, appear to vary between devices, with network traffic data being the main type of data mentioned in the cases of security systems, lighting, temperature and ventilation, occupancy-aware

control, smart plugs, automation for elderly and sick, and entertainment; audio data in the case of voice control devices; and energy usage data in the case of smart grids and readers and smart kitchens. To mention some examples, [50] analysed the eavesdropping of network traffic data from wireless cameras to identify the presence of people in the house, and [55] studied malware used to access network traffic at flow-level granularity from a variety of security, lighting and occupancy-aware devices. Other types of data not covered in Table 6 included network system information, such as access points, IP addresses, and log-in credentials. We also note that, in the case of cleaning robots, no specific type of vulnerable data was identified, but [37] analysed their insecure firmware more generally.

Table 6. Type of data that may pose vulnerabilities for each smart home device

	Network traffic	Energy usage	Written comms	Audio	Image	Video
Security and surveillance	12	3	5	1	3	3
Lighting control, smart bulb	10	3	4	1	1	1
Voice control device	4	4	2	6	2	1
Temperature and ventilation	5	4	4	1	2	2
Smart home app or browser	7	5	4	1	3	3
Occupancy-aware control	5	4	2	1	2	1
Smart plug	6	4	1	1	1	1
Automation for elderly/sick	3	1	2	2	2	2
Entertainment	3	1	2	1	2	2
WiFi	2	1	2	0	0	0
Smart kitchen	1	2	0	0	0	0
Smart grid and smart meter	0	3	0	0	0	0
Leak detector and air quality	1	1	2	1	1	1
Pet or baby care	1	0	1	0	0	0
Cleaning robot	0	0	0	0	0	0

4.4 Approaches to mitigate digital harms of smart homes

Finally, we also recorded data about the recommendations mentioned in each study to mitigate the digital harms of smart devices. 56 studies (88.9%) included explicit recommendations to mitigate digital harms. As shown in Figure 7(a), the vast majority of studies focused on technical improvements (55, 87.3%), while fewer mentioned prevention based on education (10, 15.9%) and change in policy (2, 3.2%). No study mentioned other forms of prevention, such as prevention based on control over victims or perpetrators.

Studies that focus on technical improvements, however, take highly dissimilar approaches. To mention a few examples, a variety of approaches are proposed to better identify malicious intrusions, including decision tree models [6], deep learning models that learn from time-series data [5, 26], machine learning trained from datasets of users with similar characteristics [10], automated intrusion detection systems that adapt to new threats [15, 19], and distance-based verification procedures to identify unintended pairing of IoT devices [56]. Others focus on improving the technical specification

of traffic packets to better conceal their content: [59] propose making randomly occurring deceptive connections, [4, 25] replaying fake packages and flows at random times, [31] appending randomised amounts of bytes to each connection, [23] applying differential privacy to better conceal packets, and [30] adding information about the last message sent in each packet, so devices can easily identify if a device has been corrupted. Other technical recommendations include over-the-air firmware update systems to quickly address vulnerabilities of devices [52], not allowing individual devices to freely connect themselves to the network (only through a control hub) [14], and hardware and privacy moderation algorithms to protect data [22].

Several studies also mention the need to provide training and education for users, for example, in [14], "users should be encouraged to educate themselves on the aspects of cybersecurity to increase their ability to identify and respond to cybersecurity risks within smart homes" (p. 735), with a particular focus on those with cognitive impairment and deficits in [63], social workers in [34], and developers in [39]. [27] propose more stringent regulations and certification programmes.

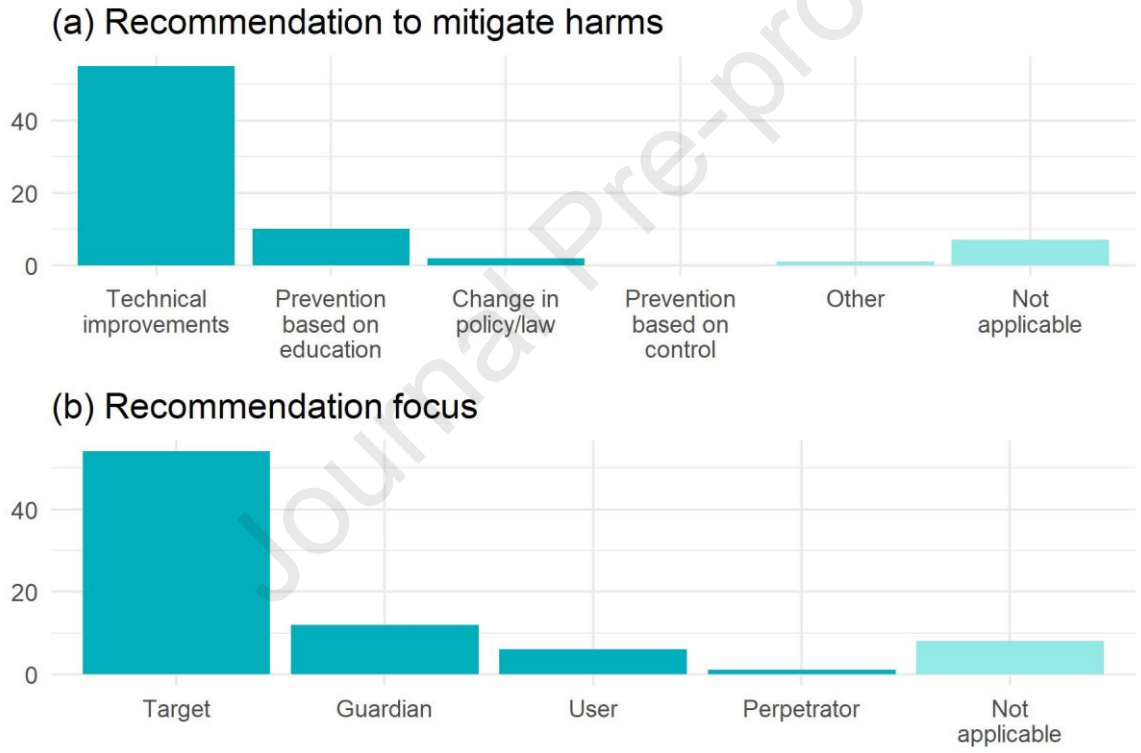

Figure 7. Recommendations to mitigate digital harms of smart devices

Most studies focus their recommendations on smart devices (54, 85.7%), while the proportion of studies that propose recommendations focused on the potential guardians (12, 19.0%), users (6, 9.5%) and perpetrators (1, 1.6%) is relatively small (Figure 7(b)). For instance, [34] focuses on the training of social workers to better assist victims of domestic abuse, and [28] argues developers and vendors should undertake ongoing threat assessments to improve the technical specifications of devices. Others propose more imaginative solutions, such as encouraging users to place moving objects (e.g., a clock) in front of smart cameras to continuously trigger the system and prevent offenders from detecting when users are not at home [25]. [34] propose multi-factor authentication systems to prevent household members from stalking each other through companion apps.

5. Discussion and conclusions

The use of smart home devices is growing rapidly across the globe. Between 2017 and 2021, the use of devices such as smart thermostats, smart TVs, and smart lighting increased by over 50% in the UK, and smart doorbells and smart speakers by over 75% (techUK, 2021). Similar trends are seen in the US, where over 65% of residents own smart devices (Harvey, 2022). With the rapid uptake of smart technologies at home, it becomes vital for developers and vendors, as well as users and policymakers, to fully understand their benefits as well as their potential risks and barriers.

While there is a growing body of academic research exploring the potential harms of smart devices, there is still an overall lack of information about the nature and extent of these harms, and no public records offer insights into this. We argue that the field is now at a point where unique studies can be synthesised to obtain a comprehensive overview of the digital harms of smart devices. Thus, this article has presented a first-of-its-kind systematic review of the privacy- and security-related harms of smart home technologies. Following the PRISMA protocol in two widely used academic databases, seven researchers selected 63 studies that met a set of inclusion criteria and extracted information from them. This systematic review offers an overview of smart home devices and attributes that may pose digital harms, classifies these digital harms, and summarises approaches to mitigate them. This review thus contributes to the growing theoretical body aimed at better understanding the adoption and implementation of IoT technologies (Nord et al., 2019). Only by synthesising existing evidence on the digital harms of smart homes can we understand the privacy and security challenges for the adoption of such technologies, and in turn develop mechanisms to mitigate such harms and enhance a safe implementation of IoT devices in home settings. Importantly, this review of the literature not only allows for a better understanding of the digital harms of smart homes, but also identifies relevant gaps in evidence and suggests directions for future research (see Table 7).

Our review identified that the majority of existing studies focus on privacy intrusions as a prevalent form of harm against smart homes. Privacy intrusions can take the form of non-criminal (e.g., uncontrolled access by medical practitioners and carers to private data recorded in care monitoring devices; Alkhatib et al., 2019) as well as criminal behaviour (e.g., when information obtained from smart homes is subsequently used to control household members or target houses for burglary; Hodges, 2021), which in turn affects the types of actions companies and law enforcement should put in place to prevent and respond to them. Other factors that influence the private and public responses to digital harms include the type of device and data linked to each harm, and the nature of the harm itself. This is the reason why in this study we recorded information not only about the most prevalent harm types, but also classified these harms and the variety of harm-affected devices.

Other types of harms that are less common in the literature include hacking, malware and DoS/DDoS attacks targeting a variety of home devices. Some of these types of attacks were also recorded in Blythe and Johnson (2021). Fewer articles studied stalking incidents, and one of them, Sikder et al. (2020), found that the way in which access control settings in smart homes are designed leads to users being granted undesired full access control to all smart home ecosystems (e.g., AirBnB guests). While the differences in the prevalence of the types of harms identified in this systematic review may indeed reflect real-world patterns, the frequencies observed here are likely affected by the overall interests of researchers and funders, and that it is easier or more convenient to study

some harm types over others. Thus, while this systematic review provides valuable information about the types of harms that researchers have so far identified, it is necessary for researchers and public authorities to work collaboratively on new ways to more accurately estimate the extent and nature of digital harms – this is identified as an important gap in research. Some consider that creating public-private partnerships for data sharing and evidence-based prevention in the context of smart homes is essential to further understand their benefits and harms, and in turn put measures in place for prevention (Buil-Gil et al., 2022).

Moreover, in order to better understand these harms and derive effective prevention mechanisms, either technical, social, or socio-technical, we argue that it is important to classify them according to their nature, methods and objectives. Our study shows how previous classifications of online harms can be applied to better understand the harms of smart homes (Lin and Bergmann, 2016; McGuire and Dowling, 2013; Wall, 2001). We found that harms identified in extant academic literature tend to cluster on incidents at the intersection of cyber-dependent, access and trespass, and cyber-dependent, confidentiality and trespass. We have seen several examples of harms with these characteristics, as presented in the academic literature as well as in known cases, but we have also seen examples of other types of harms that are either less commonly identified or fully neglected in existing research. While our systematic review is important to gain a better understanding of the nature of the harms of smart devices, it also identifies gaps in research that should be better addressed in the future. For instance, we found research gaps regarding harms at the intersection of cyber-enabled and deception, and cyber-enabled and pornography, which nonetheless do exist in the real-world (e.g., data retrieved from smart homes being used for identity theft or to assist fraud, or the dissemination of sexually explicit images of children obtained from monitoring devices).

Another key finding of this systematic review is that digital harms, and data associated with these harms, may vary extensively across smart home devices (Marikyan et al., 2019). For instance, according to data extracted from this review, while harms associated with security and surveillance systems have been mainly linked to DoS attacks and privacy intrusions arising from insufficient protection of network traffic data, voice control devices (e.g., Google Home, Amazon Alexa) are more commonly associated with the hacking of audio data. And while lighting control systems are commonly linked with the hacking of network traffic data, smart grids/meters are mainly linked to privacy intrusions of energy usage. This type of information may indeed be essential to propose and design better prevention mechanisms that adapt to the types of data vulnerabilities and harms of each specific device, user and context. In a similar vein, these findings can help inform policy and legislation such as the UK PSTI Bill.

The vast majority of studies included in our systematic review propose explicit measures to mitigate the digital harms identified. Most of these recommendations focus on technical improvements with different aims, mostly related to improving intrusion detection systems, data protection and concealment mechanisms, and software updates. Fewer mentioned hardware improvements. Previous studies also found that most studies focus on the technical prevention of harms (Blythe and Johnson, 2021). While we found a considerable proportion of studies proposing technical recommendations for harm prevention, very few articles mentioned social prevention mechanisms

such as improving the education of users or developers, and only two articles described the need for policy changes. Relatedly, most of these recommendations focused on the target, with fewer considering harm reduction and prevention from the perspective of the guardian, user or perpetrator (Leukfeldt and Yar, 2016). This article thus identifies another important gap in research: the need to consider and evaluate the effectiveness of social and socio-technical prevention approaches that focus on the guardian, user and perpetrator. The main gaps in research identified in this study, and directions for future research, are presented in Table 7.

Table 7. Main gaps in research and directions for future research

Gaps in research	Research questions
Better measurement of the nature and extent of digital harms of smart homes	Do digital harms considered in the literature reflect real-world incidents? How can we better estimate the nature and extent of digital harms of smart homes?
Digital harms at the intersection of cyber-enabled and deception	What is the nature and extent of cyber-enabled and deception-related digital harms of smart homes?
Digital harms at the intersection of cyber-enabled and porn and obscenity	What is the nature and extent of cyber-enabled and obscenity-related digital harms of smart homes?
Social prevention mechanisms (e.g., education, control, policy) against digital harms of smart homes	What are the most relevant social factors that explain the digital harms of smart homes? How can we better design social and socio-technical approaches to prevent the digital harms of smart homes?
Prevention mechanisms focused on the user, perpetrator or guardian	What is the role of the user, perpetrator and guardian in the digital harms of smart homes? How can we better design prevention mechanisms focused on the user, perpetrator or guardian?

Some of these gaps in research could, and perhaps should, be addressed through cross-disciplinary initiatives involving researchers from different fields. We have observed an overall lack of multidisciplinary work in this domain, with not a single study involving researchers from across both technical and health or social sciences disciplines. For instance, our review found evidence that while crossing physical and political boundaries does not appear to be an issue for collaborative work (i.e., 13 studies involved authors from multiple countries), crossing disciplinary boundaries appears much more challenging for researchers interested in the study of smart homes. This is likely to be the primary driver for some of the research gaps identified, including the lack of research about cyber-enabled harms, and incidents related to deception, violence and pornography, and the main focus on solely technical prevention mechanisms to improve the protection of smart devices. We argue that enhancing cross-disciplinary work in this domain is not only important to better address the wider variety of harms that affect devices, and the wider possibilities of harm reduction strategies, but to better research them. While most studies in our systematic review were described as

experimental or quasi-experimental by design, few of them consider the selection of randomised control and trial groups, which is considered a fundamental requirement for experimental designs in many disciplines. Similarly, very few studies in our review apply mixed-methods (i.e., combining quantitative and qualitative data analysis) to better understand the harms of smart homes, and not a single study applies meta-analytical designs to compare findings presented in multiple studies. Few studies considered the experiences of victims in the assessment and response to the security and privacy threats of smart homes (Leitão, 2019). As has been noted regarding the study of wearable technology (Ferreira et al., 2021), research in the field of smart homes will undoubtedly benefit from further enhancing principles of cross-disciplinarity and considering the voices of everyone involved in the design, development, and use of smart home technologies.

6. Limitations

This study, however, is not free from limitations. First, we considered two academic databases to search for academic articles for our systematic review (Web of Science and Scopus). While these are two of the most widely used databases of academic literature, not all articles are included in them, and thus we may have missed some important contributions in the field. Second, we only considered articles published between 2011 and 2021, and our study may have missed important contributions published both before and after this time period. Relatedly, the ever-changing nature of smart homes and their associated harms may mean that some of the findings identified here may vary extensively in the next few years. Third, while the process followed to select articles for our review is based on a widely adopted protocol for systematic reviews, and we considered interrater reliability criteria to ensure consistency across judges, we cannot rule out the possibility that some other relevant articles should have also been included in the study. Fourth, the exemplar cases used to illustrate our main findings were selected using non-probability purposive sampling and may not be representative of the most common types of harms occurring in the real-world. And fifth, as described in previous sections, while the digital harms identified in this review may reflect real-world patterns, these may also be driven by the overall methodological approaches and areas of interests of researchers and funders.

References

Aafer, Y., You, W., Sun, Y., Shi, Y., Zhang, X., and Yin, H. (2021). Android {SmartTVs} vulnerability discovery via {log-guided} fuzzing. In *30th USENIX Security Symposium* (pp. 2759-2776). USENIX.

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., and Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1), tyy006.

Ali, W. Dustgeer, G., Awais, M., and Shah, M.A. (2017). IoT based smart home: security challenges, security requirements and solutions. In *23rd International Conference on Automation and Computing* (pp. 1-6). IEEE.

Alkhatib, S., Waycott, J., and Buchanan, G. (2019). Privacy in aged care monitoring devices (ACMD): The developers' perspective. In E. Cummings, M. Merolli and L.K. Schaper (Eds.), *Digital health: Changing the way healthcare is conceptualised and delivered* (pp. 7-12). Amsterdam: IOS Press.

AlOtaibi, N., and Lombardi, F. (2021). Privacy and security evaluation of Amazon Echo voice assistant. In *2021 International Conference of Women in Data Science at Taif University* (pp. 1-6). IEEE.

Alsheakh, H., and Bhattacharjee, S. (2020). Towards a unified trust framework for detecting IoT device attacks in smart homes. In *IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems* (pp. 613-621). IEEE.

Anthi, E., Ahmad, S., Rana, O., Theodorakopoulos, G., and Burnap, P. (2018). EclipseIoT: A secure and adaptive hub for the Internet of Things. *Computers & Security*, 78, 477-490.

Anthi, E., Williams, L., Javed, A., and Burnap, P. (2021). Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. *Computers & Security*, 108, 102352.

Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2805.

BBC (2013, September 5). *Trendnet ruling heralds crackdown on insecure home webcams*. Available from: https://www.bbc.com/news/technology-23971118 (Accessed 2 August 2022).

BEIS (2022). *Smart meters in Great Britain, quarterly update March 2022*. Available from: https://www.gov.uk/government/statistics/smart-meters-in-great-britain-quarterly-update-march-2022 (Accessed 10 August 2022).

Bhatt, P., and Morais, A. (2018). HADS: Hybrid anomaly detection system for IoT environments. In *2018 International Conference on Internet of Things, Embedded Systems and Communications* (pp. 191-196). IEEE.

Birchley, G., Huxtable, R., Murtagh, M., Meulen, R., Flach, P., and Gooberman-Hill, R. (2017). Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies. *BMC Medical Ethics*, 18(23), 1-13.

Bistarelli, S., Bosimini, E., and Santini, F. (2020). A report on the security of home connections with IoT and docker honeypots. In M. Loreti and L. Spalazzi (Eds.), *Proceedings of the Fourth Italian Conference on Cyber Security* (pp. 60-70). CEUR.

Blythe, J.M., and Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 34, 97-125.

Boise, L., Wild, K., Mattek, N., Ruhl, M., Dodge, H.H., and Kaye, J. (2013). Willingness of older adults to share data and privacy concerns after exposure to unobtrusive in-home monitoring. *Gerontechnology*, 11(3), 428-435.

Bordel, B., Alcarria, R., Robles, T., and Sánchez-Picot, Á. (2018). Stochastic and information theory techniques to reduce large datasets and detect cyberattacks in ambient intelligence environments. *IEEE Access*, 6, 34896-34910.

Bugeja, J., Jacobsson, A., and Spalazzese, R. (2020). On the analysis of semantic denial-of-service attacks affecting smart living devices. In K. Arai, S. Kapoor and R. Bhatia (Eds.), *Intelligent Computing: Proceedings of the 2020 Computing Conference*, Volume 2 (pp. 427-444). Cham: Springer.

Buil-Gil, D., Nicholson, J., and Kemp, S. (2022). *Smart (and safe) homes – public-private partnerships to mitigate the digital harms of smart home devices*. Policy@Manchester blog. Available from: https://blog.policy.manchester.ac.uk/posts/2022/03/smart-and-safe-homes-public-private-partnerships-to-mitigate-the-digital-harms-of-smart-home-devices/ (Accessed 6 August 2022).

Capellupo, M., Liranzo, J., Bhuiyan, M.Z.A., Hayajneh, T., and Wang, G. (2017). Security and attack vector analysis of IoT devices. In G. Wang, M. Atiquzzaman, Z. Yan and K.R. Choo (Eds.), *Security, privacy and anonymity in computation, communication, and storage: SpaCCS 2017 international workshops* (pp. 593-606). Cham: Springer.

Choi, Y.K., Thompson, H. J., Demiris, G. (2021). Internet-of-things smart home technology to support aging-in-place: Older adults' perceptions and attitudes. *Journal of Gerontological Nursing*, 47(4), 15-21.

Copos, B., Levitt, K., Bishop, M., and Rowe, J. (2016). Is anybody home? Inferring activity from smart home network traffic. In *2016 IEEE Security and Privacy Workshops* (pp. 245-251). IEEE.

Corbett, J. (2013). Using information systems to improve energy efficiency: Do smart meters make a difference? *Information Systems Frontiers*, 15, 747-760.

Crime Prosecution Service (n.d.). *Cyber / online crime.* Available from: https://www.cps.gov.uk/crime-info/cyber-online-crime (Accessed 29 July 2022).

Cultice, T., Ionel, D., and Thapliyal, H. (2020). Smart home sensor anomaly detection using convolutional autoencoder neural network. In *2020 IEEE International Symposium on Smart Electronic Systems* (pp. 67-70). IEEE.

Demiris, G., and Hensel, B.K. (2008). Technologies for an aging society: A systematic review of "smart home" applications. *Yearbook of Medical Informatics*, 17(1), 33-40.

DCMS (2019). *Online Harms White Paper*. Available from: https://www.gov.uk/government/consultations/online-harms-white-paper (Accessed 2 August 2022).

DCMS (2021a). *Product Security and Telecommunications Infrastructure (PSTI) Bill: Factsheets.* Available from: https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets (Accessed 2 August 2022).

DCMS (2021b). *Draft Online Safety Bill*. Available from: https://www.gov.uk/government/publications/draft-online-safety-bill (Accessed 2 August 2022).

Do, Q., Martini, B., and Choo, K. R. (2018). Cyber-physical systems information gathering: A smart home case study. *Computer Networks*, 138, 1-12.

Dorri, A., Kanhere S.S., Jurdak, R., and Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 618-623). IEEE.

Fan, J., Li, Q., and Cao, G. (2017). Privacy disclosure through smart meters: Reactive power based attack and defense. In *47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (pp. 13-24). IEEE.

Ferreira, J.J., Fernandes, C.I., Rammal, H.G., Veiga, P.M. (2021). Wearable technology and consumer interaction: A systematic review and research agenda. *Computers in Human Behavior*, 118, 106710.

Gassais, R., Ezzati-Jivan, N., Fernandez, J.M., Aloise, D., and Dagenais, M.R. (2020). Multi-level host-based intrusion detection system for Internet of things. *Journal of Cloud Computing*, 9, 62.

Han, J., and Park, T. (2017). Security-enhanced push button configuration for home smart control. *Sensors*, 17(6), 1-18.

Hariri, A., Giannelos, N., and Arief, B. (2020). Selective forwarding attack on IoT home security kits. In S. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, C. Kalloniatis, J. Mylopoulos, A. Antón, S. Gritzalis, F. Pallas, J. Pohle, A. Sasse, W. Meng, S. Furnell and J. Garcia-Alfaro (Eds.), *Computer security: ESORICS 2019 international workshops, CyberICPS, SECPRE, SPOSE, and ADIoT* (pp. 360-373). Cham: Springer.

Harvey, A. (2022). *American home tech spending survey 2022*. Safewise. Available from: https://www.safewise.com/blog/smart-home-tech-spending/ (Accessed 5 August 2022).

Heartfield, R., Loukas, G., Bezemskij, A., and Panaousis, E. (2021). Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning. *IEEE Transactions on Information Forensics and Security*, 16, 1720-1735.

Hodges, D. (2021). Cyber-enabled burglary of smart homes. *Computers & Security*, 110, 102418.

Isawa, R., Ban, T., Tie, Y., Yoshioka, K., and Inoue, D. (2018). Evaluating disassembly-code based similarity between IoT malware samples. In *13th Asia Joint Conference on Information Security* (pp. 89-94). IEEE.

Jacobsson, A., Bold, M., and Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, 56, 719-733.

Javed, Y., and Rajabi, N. (2020). Multi-layer perceptron artificial neural network based IoT botnet traffic classification. In K. Arai, R. Bhatia and S. Kapoor (Eds.), *Proceedings of the future of technologies conference (FTC) 2019*, Volume 1 (pp. 973-984). Cham: Springer.

Javed, A., Malik, K.M., Irtaza, A., and Malik, H. (2021). Towards protecting cyber-physical and IoT systems from single- and multi-order voice spoofing attacks. *Applied Acoustics*, 183, 108283.

Ji, W., Cheng, Y., Xu, W., and Zhou, X. (2018). User presence inference via encrypted traffic of wireless camera in smart homes. *Security and Communication Networks*, 2018, 1-10.

Jia, Y., Xiao, Y., Yu, J., Cheng, X., Liang, Z., and Wan, Z. (2018). A novel graph-based mechanism for identifying traffic vulnerabilities in smart home IoT. In *IEEE INFOCOM 2018: IEEE Conference on Computer Communications* (pp. 1493-1501). IEEE.

Kennedy, S., Li, H., Wang, C., Liu, H., Wang, B., and Sun, W. (2019). I can hear your Alexa: Voice command fingerprinting on smart home speakers. In *2019 IEEE Conference on Communications and Network Security* (pp. 232-240). IEEE.

Komninos, N., Philippou, E., and Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4), 1933-1954.

Krebs, B. (2017). *Who is Anna-Senpai, the Mirai Worm Author?* Available from: https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/ (Accessed 30 July 2022).

Lally, G., and Sgandurra, D. (2018). Towards a framework for testing the security of IoT devices consistently. In A. Saracino and P. Mori (Eds.), *Emerging technologies for authorization and authentication: First international workshop, ETAA 2018* (pp. 88-102). Cham: Springer.

Laufs, J., Borrion, H., and Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, 55, 102023.

Lee, B., Kwon, O., Lee, I., and Kim, J. (2017). Companionship with smart home devices: The impact of social connectedness and interaction types on perceived social support and companionship in smart homes. *Computers in Human Behavior*, 75, 922–934.

Leitão, R. (2019). Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (p. 527-539). New York: ACM.

Leukfeldt, E.R., and Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263-280.

Li, J., Li, Z., Tyson, G., and Xie, G. (2020). Your privilege gives your privacy away: An analysis of a home security camera service. In *IEEE Conference on Computer Communications* (pp. 387-396). IEEE.

Li, Y., Zhang, Y., Zhu, H., and Du, S. (2021). Toward automatically generating privacy policy for smart home apps. In *IEEE Conference on Computer Communications Workshops* (pp. 1-7). IEEE.

Lin, H., and Bergmann, N.W. (2016). IoT privacy and security challenges for smart home environments. *Information*, 7, 44.

Lutolf, R. (1992). Smart Home concept and the integration of energy meters into a home based system. In *Seventh International Conference on Metering Apparatus and Tariffs for Electricity Supply* (pp. 277-278). IEEE.

Lyu, M., Sherratt, D., Sivanathan, A., Gharakheili, H., Radford, A., and Sivaraman, V. (2017). In *WiSec '17: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 46-51). New York: ACM.

Mahadewa, K.T., Wang, K., Bai, G., Shi, L., Dong, J.S., and Liang, Z. (2018). HOMESCAN: Scrutinizing implementations of smart home integrations. In *2018 23rd International Conference on Engineering of Complex Computer Systems* (pp. 21-30). IEEE.

Marikyan, D., Papagiannidis, S., and Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*, 138, 139–154.

Martin, E. D., Kargaard, J., and Sutherland, I. (2019). Raspberry Pi malware: An analysis of cyberattacks towards IoT devices. In *10th International Conference on Dependable Systems, Services and Technologies* (pp. 161-166). IEEE.

Mashima, D., Serikova, A., Cheng, Y., and Chen, B. (2018). Towards quantitative evaluation of privacy protection schemes for electricity usage data sharing. *ICT Express*, 4(1), 35-41.

Matern, D., Condurache, A., and Mertins, A. (2013). Adaptive and automated ambiance surveillance and event detection for Ambient Assisted Living. In *35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (pp. 7318-7321). IEEE.

McGuire, M., and Dowling, S. (2013). *Cyber crime: A review of the evidence*. Home Office Research Report 75. London: Home Office.

Min, B., and Varadharajan, V. (2016). Design and evaluation of feature distributed malware attacks against the Internet of Things (IoT). In *20th International Conference on Engineering of Complex Computer Systems* (pp. 80-89). IEEE.

Mohler, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L.A., and PRISMA-P Group (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic Reviews*, 4, 1.

de Morais, W. O., Lundström, J., and Wickström, N. (2014). Active in-database processing to support ambient assisted living systems. *Sensors*, 14(8), 14765-14785.

Nicholls, L., Strengers, Y., and Sadowski, J. (2020). Social impacts and control in the smart home. *Nature Energy*, 5, 180-182.

Nord, J.H., Koohang, A., and Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, 133(1), 97-108.

Oconnor, T.J., Jessee, D., and Campos, D. (2021). Through the spyglass: Towards IoT companion app man-in-the-middle attacks. In *CSET '21: Cyber Security Experimentation and Test Workshop* (pp. 58-62). New York: ACM.

Peng, P., and Wang, A. (2020). SmartMon: Misbehavior detection via monitoring smart home automations. In *IEEE/ACM Symposium on Edge Computing* (pp. 327-333). IEEE.

Piasecki, S., Urquhart, L., and McAuley, P.D. (2021). Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards. *Computer Law & Security Review*, 42, 105542.

Rauti, S., Laato, S., and Pitkämäki, T. (2021). Man-in-the-browser attacks against IoT devices: A study of smart homes. In A. Abraham, Y. Ohsawa, N. Gandhi, M. A. Jabbar, A. Haqiq, S. McLoone and B. Isaac (Eds.), *Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition* (pp. 727-737). Cham: Springer.

Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., and Logé, C. (2006). The smart home concept: Our immediate future. In *1st IEEE International Conference on E-Learning in Industrial Electronics* (pp. 23-28). IEEE.

Salomons, E., Sela, L., Housh, M. (2020). Hedging for privacy in smart water meters. *Water Resources Research*, 56(9), e2020WR027917.

Sikder, A.K., Babun, L., Aksu, H., and Uluagac, A.S. (2019). Aegis: a context-aware security framework for smart home systems. In *Proceedings of the 35th Annual Computer Security Applications Conference* (pp. 28-41). New York: ACM.

Sikder, A.K., Babun, L., Celik, Z.B., Acar, A., Aksu, H., McDaniel, P., Kirda, E., Uluagac, A.S. (2020). Kratos: multi-user multi-device-aware access control system for the smart home. In *WiSec '20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 1-12). New York: ACM.

Sivanathan, A., Sherratt, D., Gharakheili, H., Sivaraman, V., and Vishwanath, A. (2017). Low-cost flow-based security solutions for smart-home IoT devices. In *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems* (pp. 1-6). IEEE.

Sivanathan, A., Loi, F., Gharakheili, H., and Sivaraman, V. (2018). Experimental evaluation of cybersecurity threats to the smart-home. In *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems* (pp. 1-6). IEEE.

Skowron, M., Janicki, A., and Mazurczyk, W. (2020). Traffic fingerprinting attacks on Internet of Things using machine learning. *IEEE Access*, 8, 20386-20400.

Sovacool, B.K., & Furszyfer Del Rio, D.D. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and Sustainable Energy Reviews*, 120, 109663.

techUK (2021). *The state of the connected home 2021: A year like no other*. Available from: https://spark.adobe.com/page/LCRPh1X14fjDM/ (Accessed 11 August 2021).

Teng, C.C., Gong, J.W., Wang, Y.S., Chuang, C.P., and Chen, M.C. (2017). Firmware over the air for home cybersecurity in the Internet of Things. In *19th Asia-Pacific Network Operations and Management Symposium* (pp. 123-128). IEEE.

Tran, B., Pan, S., Liang, X., and Zhang, H. (2021). Exploiting physical presence sensing to secure voice assistant systems. In *IEEE International Conference on Communications* (pp. 1-6). IEEE.

Tushir, B., Dalal, Y., Dezfouli, B., and Liu, Y. (2021). A quantitative study of DDoS and E-DDoS attacks on WiFi smart home devices. *IEEE Internet of Things Journal*, 8(8), 6282-6292.

Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Future Research*, 4, 18.

Ullrich, F., Classen, J., Eger, J., and Hollick, M. (2019). Vacuums in the cloud: Analyzing security in a hardened IoT ecosystem. In *13th USENIX Workshop on Offensive Technologies*. USENIX.

US Department of Justice (2017). *Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant Cyber Attacks*. U.S. Attorney's Office. Available from: https://www.justice.gov/usao-nj/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases (Accessed 2 August 2022).

Vidal-González, S., García-Rodríguez, I., Aláiz-Moretón, H., Benavides-Cuéllar, C., Benítez-Andrades, J.A., García-Ordás, M.T., and Novais, P. (2020). Analyzing IoT-based botnet malware activity with distributed low interaction honeypots. In A. Rocha, H. Adeli, L.P. Reis, S. Costanzo, I. Orovic and F. Moreira (Eds.), *Trends and innovations in information systems and technologies*, Volume 2 (pp. 329-338). Cham: Springer.

Wall, D. (2001). *Crime and the Internet*. New York: Routledge.

Wan, Y., Xu, K., Wang, F., and Xue, G. (2021). IoTAthena: Unveiling IoT device activities from network traffic. *IEEE Transactions on Wireless Communications*, 21(1), 651-664.

Wang, C., Kennedy, S., Li, H., Hudson, K., Atluri, G., Wei, X., Sun, W., Wang, B. (2020). Fingerprinting encrypted voice traffic on smart speakers with deep learning. In *WiSec '20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 254-265). New York: ACM.

Wang, Q., Ji, S., Tian, Y., Zhang, X., Zhao, B., Kan, Y., Lin, Z., Lin, C., Deng, S., Liu, A. X., and Beyah, R. (2021). {MPInspector}: A systematic and automatic approach for evaluating the security of {IoT} messaging protocols. In *30th USENIX Security Symposium* (pp. 4205-4222). USENIX.

Wang, Y., Li, X., Jia, P., Yang, Y., and Wang, H. (2021). Sensitive instruction detection based on the context of IoT sensors. In *51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops* (pp. 121-128). IEEE.

Weber, R.H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23-30.

Xiao, Y., Jia, Y., Liu, C., Alrawais, A., Rekik, M., and Shan, Z. (2020). HomeShield: A credential-less authentication framework for smart home systems. *IEEE Internet of Things Journal*, 7(9), 7903-7918.

Yamauchi, M., Ohsita, Y., and Murata, M. (2021). Platform utilizing similar users' data to detect anomalous operation of home IoT without sharing private information. *IEEE Access*, 9, 130615-130626.

YouGov (2020). *The dawn of the connected home*. Available from: https://yougov.co.uk/topics/technology/articles-reports/2020/08/27/smart-speakers-no-longer-just-early-adopters (Accessed 3 August 2022).

Yu, X., Zhang, Y., Li, X. Y., and Guo, X. (2021). The Truman show: Attack on the privacy of smart home through traffic analysis. In *7th International Conference on Big Data Computing and Communications* (pp. 121-128). IEEE.

Zainab, A., Refaat, S.S., and Bouhali, O. (2020). Ensemble-based spam detection in smart home IoT devices time series data using machine learning techniques. *Information*, 11(7), 344.

Zhang, W., Meng, Y., Liu, Y., Zhang, X., Zhang, Y., and Zhu, H. (2018). HoMonit: Monitoring smart home apps from encrypted traffic. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1074-1088). New York: ACM.

Zhang, B., Li, J., Zheng, X., Ge, J., and Sun, J. (2019). A blockchain-based mobile IOT network interconnection security trusted protocol model. In J. Vaidya, X. Zhang and J. Li (Eds.), *Cyberspace safety and security: 11th international symposium* (pp. 372-381). Cham: Springer.

Highlights

- With the rapid uptake of smart home technologies, it becomes vital to fully understand their benefits, risks and barriers.
- Privacy intrusions are the most common type of harm identified in the literature, followed by hacking, malware and DoS.
- Smart homes may also enable new forms of cyberstalking and exacerbate power asymmetries between the household members.
- It is necessary to find new ways to accurately estimate the extent and nature of the digital harms of smart devices.
- Gaps in research should be addressed through cross-disciplinary initiatives involving researchers from different fields.

The authors have no conflicts of interest to declare.