Future Generation Computer Systems 149 (2023) 664–678

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Complex online harms and the smart home: A scoping review

Shola Olabode [a,*], Rebecca Owens [b], Viana Nijia Zhang [c], Jehana Copilah-Ali [d], Maxim Kolomeets [c,e], Han Wu [f], Shrikant Malviya [e], Karolina Markeviciute [g], Tasos Spiliotopoulos [f], Cristina Neesham [d], Lei Shi [c], Deborah Chambers [a]

[a] School of Arts and Cultures, Newcastle University, Newcastle Upon Tyne, NE1 7RU, UK
[b] Newcastle Law School, Newcastle University, Newcastle Upon Tyne, NE1 7RU, UK
[c] School of Computing, Newcastle University, Newcastle Upon Tyne, NE1 7RU, UK
[d] Business School, Newcastle University, Newcastle Upon Tyne, NE1 7RU, UK
[e] Department of Computer Science, Durham University, Durham, DH1 3LE, UK
[f] School of Computer Science, University of Birmingham, Birmingham, B15 2TT, UK
[g] Business School, Durham University, Durham, DH1 3LE, UK

ARTICLE INFO

Article history:
Received 1 March 2023
Received in revised form 7 August 2023
Accepted 14 August 2023
Available online 18 August 2023

Keywords:
Smart homes
Complex online harms
Privacy risks
Security vulnerabilities
Law
Ethics

ABSTRACT

Background: Technological advances in the smart home have created new opportunities for supporting digital citizens' well-being and facilitating their empowerment but have enabled new types of complex online harms to develop. Recent statistics have indicated that 'smart' technology ownership increases yearly, driven by lower costs and increased accessibility. Research on smart homes has also grown, focusing on technology perspectives at the expense of a user-centric approach sensitive to the smart home's harms, risks, and vulnerabilities.
Objective: This scoping review addresses the information gap by underscoring the scope of literature that exists regarding complex online harms, vulnerabilities, and risks associated with smart home technologies and citizens' agency. The goal is to understand the state of knowledge, gaps in the literature, and areas for future study. The importance and originality of this paper lie in its interdisciplinary review and approach. It is hoped that this research will contribute to a deeper understanding of complex online harms in the smart home.
Design: Three online databases were utilised to identify papers published between 2017 and 2022, from which we selected 235 publications written in English that addressed harms, risks, vulnerabilities, and agency in the smart home context. This allowed us to map contemporary literature to reveal significant gaps in our understanding of the complex online harms affecting smart home users and identify opportunities for further research.
Results: This review identified emerging themes of 'risks', 'vulnerabilities', and 'harms' in that order of frequency within the literature on smart homes. The usage of terms is skewed towards computing science and information security, which comprised the majority of the literature at 54.6%. Human–computer interaction papers contributed 24.4%, while social sciences accounted for 16.2%.
Conclusion: Risks, harms and vulnerabilities within smart home ecosystems and IoTs are ongoing issues with complexities that necessitate research. Privacy, security, and well-being are key themes that embody the scope of complex harms affecting smart home devices in the broad literature. This review establishes disciplinary research gaps, especially in user-centred perspectives, due to a heavy technology focus in the existing literature. Therefore, further research is needed to address emergent risks, harms and vulnerabilities of smart home devices and understand how user agency and autonomy can complement the design, interface, and socio-technical aspects of smart home systems.

1. Introduction

The digital world offers fresh opportunities to develop innovative technologies that can enhance the wellness of citizens and contribute to the construction of healthy, happy lives [1,2]. The development of Internet of Things (IoT) connected devices has increased across various aspects of our personal and professional lives [3] and led to the growth of the smart home industry and the diversification of smart technology [4]. Throughout this paper, we utilise the term smart home to indicate a digital technology-equipped domestic residence whose occupants

* Corresponding author.
E-mail address: Shola.Olabode@newcastle.ac.uk (S. Olabode).

https://doi.org/10.1016/j.future.2023.08.019

experience conveniences, entertainment, and securities within the home and with the outside world via direct or indirect interactions and management of the technologies and systems [5]. Research indicates that the low cost and increased accessibility have dramatically increased ownership of smart home devices across various demographics [6]. It is forecast that by 2027 there will be 29.7 million smart home households in the UK, 93.6 million in the US and 164.9 million in China.[1] Whilst this technology has the potential to benefit society, it may also increase exposure to new and complex online harms, risks and vulnerabilities that digital citizens lack the agency to navigate [7,8].

This paper defines digital citizen agency as the key attribute of an individual who actively engages in awareness and their ability to initiate causal actions, produce effects and control their consequences in the smart home context [9,10]. The current design of technologies has empowered IoT devices with increasing autonomy and online agency to decide their actions when interacting with human users [10,11]. The outcome is that interconnected smart home devices collect a wide range of data from end users' homes, forming a complex environment where people may lack technical understanding of data storage, sharing, and collection [12]. This digital illiteracy can lead to digital citizens being unable to mitigate complex online harms. Therefore, by adopting the concept of 'agency' as an analytical tool to assess smart-home-based harms, risks, and vulnerabilities addressed in existing literature, this paper guides future articulations of the agency's role in empowering citizens as digital agents and promoting responsible digital social innovation of smart home-related technology.

Against this backdrop, this scoping review aims to uncover the unintended consequences of smart homes' risks, vulnerabilities and complex harms. This paper approaches the spectrum of risks, vulnerabilities and complex harms by framing the smart home user as a digital citizen in a complex adaptive system where the impact of unintended consequences is fluid [13–15]. From this perspective, risk represents the potential negative consequences or threats to the system or human users in the smart home setting due to the low resilience to privacy and security performances or capabilities [16]. In comparison, vulnerabilities are issues that pose threats or attacks to smart home technologies or systems [17]. This study also utilises the term 'complex harms' to encapsulate the multifaceted nature of harm, which transcends the traditional perpetrator/victim model to incorporate multiple stakeholders. This terminological choice was inspired by the UK Government's White Paper on Online Harm and the corresponding Online Harms Bill. As such, it recognises the intersectional nature of harm and the diverse nature of user experiences [18].

A scoping review is recognised as one of the most appropriate tools for evaluating literature that covers an emerging and broad field of work [19]. It is a practical evidence synthesis approach that adopts rigorous and transparent methods to identify knowledge gaps, scopes a body of literature and investigates research techniques [20]. Hence, this approach is particularly appropriate to examine a technologically adaptable area like smart homes. According to Wang, MacGill and Klobas [21], the potential risks surrounding adopting smart home devices are understudied. There is also a need for a comprehensive synthesis of the risks, harms and vulnerabilities in the field of Smart Home technologies [22]. This scoping review revealed a growing area of study in Computing Science and Information Security, Human-Computer Interaction, Law and Policy, Social Sciences, and Business Studies. The review identified emerging themes of 'risks', 'vulnerabilities', and 'harms', in that order of frequency, which are prevalent across these fields and require attention from researchers and practitioners alike. Due to common terminology across areas, this scoping review aims to unpack these multidisciplinary perspectives on complex online harms and outline the opportunities for these approaches to learn from one another and work together. A scoping review on complex online harms (risks, vulnerabilities, harms) of smart homes allows digital social innovation to be evaluated responsibly and facilitates the fulfilment of the UN Sustainable Development Goal 10, which aims to reduce inequalities. It has previously been found that a shared language classification around smart homes is a core starting point for reducing inequalities, as smart homes tend to 'draw on multiple social and technical disciplines that share a broad vision. However, there is a lack of interpretational consistency due to the terminology used which creates ambiguity and limits the usefulness of the evidence base in determining optimal ways to integrate technologies and housing design to meet diverse needs [23].

Contemporary literature indicates a notable lack of studies investigating the multifaceted nature of user interaction and experiences within the smart home [24]. As a result, it remains unclear what information is available about these complex online harms and their relationship to smart home technology. Addressing this gap provides the opportunity to give agency to smart home users by reducing risks and inequalities through the empowerment from passive recipients of technological services to enable digital citizens to become aware and actively engage in the decision-making processes of the smart home industry and the government [13]. This paper provides a scoping review of research on risks, harms and vulnerabilities in the context of smart homes that conforms with the Preferred Reporting Items for Systematic reviews and Meta-Analyses Extension for Scoping Reviews (PRISMA-ScR) guidelines [25]. Its primary objective is to map existing literature from a multidisciplinary perspective, identify gaps within the literature and explore opportunities for future research. This review aims to provide the foundations for a more detailed systematic review of smart home literature and form the basis of future outputs that inform the design of smart home technologies and guide technology-conscious policy-making. The following research questions guided this review:

1. *How are smart home harms/risks/vulnerabilities conceived and investigated in different disciplines of literature?*
2. *How is digital agency undermined and obtained in the smart home environment?*

This paper is organised into five main sections. Section 2 provides an overview of the methods employed for conducting the scoping review, outlining the five stages (guided by the methodological framework developed by Arksey and O'Malley [26]) involved in paper collection, selection and analysis of results. Section 3 describes the results of papers analysis using statistical, data science and analytical methods. Following this, Section 4 discusses the findings, including research limitations and recommendations for future research. Finally, in Section 5, the paper concludes with concluding remarks.

2. Research methodology

The main focus of the scoping review is to research the literature to understand the state of knowledge, methods, gaps and future research directions on the risks, vulnerabilities and harms associated with the smart home from a multidisciplinary background.

Several research methods systematically review the existing literature, including state-of-the-art and systematic reviews of contextual and more traditional approaches. However, given the aim of this paper, a scoping review represents a suitable methodology as it offers a window into the extent of research on a

[1] https://www.statista.com/outlook/dmo/smart-home/worldwide

given subject. In particular, scoping reviews are often deployed to establish the depth of knowledge about a subject, existing gaps, and possibilities for future research [27,28]. In the present context, we set out to understand the key vulnerabilities, harms, and risks emergent within the smart home's ecosystems through a multidisciplinary perspective. This is a novel area, with developments in the complexities of smart home systems complementing emerging research about the phenomenon. This review offers a platform for a broad overview of the subject across diverse fields researching the subject. Its goal is to map research concepts, ideas, definitions, sources, and categories of evidence characteristic of the multidisciplinary nature of smart home research. Notably, scoping reviews allow us to produce an overall map of what evidence has been produced as opposed to the approach associated with systematic reviewing where the best evidence available is sought to answer a tightly defined question related to policy and/or practice [28]. The subject of enquiry can be novel or long-standing with complexities or continuities in innovation. Although an in-depth examination focus goes beyond the emphasis of scoping reviews, the approach's capacity to systematically map the literature on a subject or field helps unveil trends that could inform new lines of inquiry drawing on broadly framed research questions and objectives. The five-step methodological framework developed by Arksey and O'Malley [26] guided this scoping review and informed every stage of the process:

1. Identifying the Research Question;
2. Identifying Relevant Studies;
3. Selecting Studies to Be Included in the Review;
4. Charting the Data;
5. Collating, Summarising, and Reporting the Results.

The design and methods for this scoping review comply with the PRISMA-ScR reporting guidance [25]. In addition, eligibility criteria were informed using the SPIDER guidelines [29]. Below is an overview of each stage involved in the review process.

2.1. Stage 1 – identifying the research question

The protocol was drafted using the Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols (PRISMA-P) Statement to comply with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews (PRISMA-ScR). It was developed and revised with a team of researchers with expertise in social science and humanities, human–computer interaction, business, and law. This team of research associates was drawn from a broader multidisciplinary research group, AGENCY: Assuring Citizen Agency in a World with Complex Online Harms, which aims to investigate online harms and agency. Alongside the research associates, the broader group advised on the objectives and research questions to guide the scoping review process, including search terms and keywords, synthesising and reporting findings, and databases.

The first stage of the review involved designing and identifying research questions following rigorous discussions, seminars, and workshops on smart homes across disciplinary boundaries. This process helped contextualise the research by connecting field-specific discourse about smart homes to the broader themes of agency and online harm. As a result of those deliberations with experts, research questions were identified in line with the study's objective. This is a crucial stage of the scoping review since the process of conducting a scoping review is often iterative, requiring a reflexive approach to each stage as the researcher becomes increasingly familiar with the literature, there is a possibility that revisions may be made to the research questions [28]. As part of this process, a smart home research protocol was developed and registered with the Open Science Framework on December 11, 2022.

Following multidisciplinary discussions during a series of workshops, five research questions were identified, and then two were later conscripted to inform the scoping review. These are:

1. How are smart home harms/risks/vulnerabilities conceived and investigated in different disciplines of literature?
2. How is digital agency undermined and obtained in the smart home environment?

2.2. Stage 2 – identifying relevant studies: key themes, instruments, studies, data sources and search strategy

With these research questions in mind, the researchers on the project, through workshops and seminars, deliberated on the objectives and research questions and identified the keywords that informed the search strategy and identification of relevant literature on smart homes. Initial search tests using the term online harms yielded few results. Hence the deployment of risks and vulnerabilities, as our findings support, are used fluidly to depict complex online harms in the broader literature. These keywords/ themes also reflect the multidisciplinary specificities to be drawn from searches and allow for using the concepts interchangeably especially given the diverse disciplinary lenses on smart homes.

Before proceeding with the database search, we consulted with a librarian at Newcastle University to review our search protocol and approach. Following their suggestions, they formulated a comprehensive search strategy for identifying key literature on complex online harms and smart homes. Agreed inclusion and exclusion criteria also guided the framework for the search strategy. To streamline the data management process, we used Rayyan,[2] a reliable tool for effectively organising and handling the data obtained through our search [30]. This facilitated collaborative working across our multidisciplinary research team, allowing several researchers in this study to synchronously map studies after importing the extracted research data into the software.

Following identifying key themes, the researchers agreed on choosing research databases to extract data relevant to smart homes. Three electronic databases: Scopus, Web of Science, and Westlaw, were identified as the relatively comprehensive information sources and data collection platforms considering the project's interdisciplinary nature. These platforms have some of the world's largest emerging research, archived historical and ongoing research, conference proceedings and grey literature.

To narrow down our data scope, we conducted a comprehensive review of the latest literature on smart homes, focusing on publications between 2017 and 2022. This time frame allows us to capture the most recent developments in the field over the last demi-decade. Since the subject of smart systems and their associated online harms is still emerging, we specifically sought out contemporary literature that delves into these complexities and their impact on users.

Initial steps undertaken involved a restricted search of one online database relevant to the topic to refine our methodological approach. This search resulted in 676 studies. It was determined that the advanced search must include the year of publication $>$ 2016, the term *'smart home'* and one of the terms *'vulnerability'*, *'harm'*, *'risk'* or *'agency'* mentioned in the title, abstract or keywords.

[2] https://www.rayyan.ai/

2.3. Stage 3 – selecting studies: eligibility criteria and study selection process

In this research, we leverage the following criteria based on SPIDER Tool [29] to select papers for further analysis:

- (S) Sample: All human and non-human elements involved in the interactions of the smart home context.
- (PI) Phenomenon: The phenomenon of Interest: the agency, vulnerabilities, risks, and harms resulting from developing smart home technologies.
- (D) Design: Published literature of any research design and grey literature whose quality will be evaluated by researchers.
- (E) Evaluation: Characteristics, experiences, discussions/representations of risk, vulnerabilities, and harms, aims of the paper, methods employed, key contributions of the paper and opportunities for future research.
- (R) Research type: Qualitative, quantitative, and mixed methods peer-reviewed studies. Grey literature, including third-sector and government reports and briefings, educational theses, and conference proceedings.

Thus, to be included in the scoping review, papers needed to measure or focus on specific dimensions of vulnerabilities, risks, harms, and smart homes (ecosystem, devices, technology, policy, stakeholders, users, perceptions, attitudes, adoption intentions). Also, the focus was on papers published between 2017–2022 and written in English. Studies were not limited to research methods and included quantitative, qualitative, mixed-method studies, experiments, and simulations to encompass a multidisciplinary understanding of contemporary literature.

The focus of selected smart home papers included those which addressed 'vulnerability/ies', 'risk(s)', and 'harm(s)', within the smart homes ecosystem. Smart homes also served as the boundary, and papers on domestic smart homes and assisted living facilities for the elderly were included. In contrast, papers on wearables and smart health devices were excluded, as were studies focusing on minors.

The diagram in Fig. 1 demonstrates the different mapping stages of the scoping review and is further explained below.

Three reviewers (SO, RO, and VNZ) searched information sources independently, facilitated by grading each eligibility criterion as eligible/not eligible/potentially eligible. Once the initial eligibility criteria were decided, the research articles were imported into the Rayyan database. The three lead reviewers and the data analysis team excluded articles unrelated to PI based on their titles and abstracts.

At least three team members at this stage voted to decide whether to include an article. In instances of conflict, all team members discussed if it should be included, excluded, or marked as 'maybe' for the following selection round. For studies considered potentially relevant when they cannot be excluded, the full text of a research paper was reviewed independently by at least two team members and decided based on its abstract and keywords. An article was included when both reviewers independently assessed it as satisfying the inclusion criteria from the text. The third reviewer of the data analysis team mediated in the event of disagreement following the discussion.

2.4. Stage 4 – charting the data: Categories of papers

To take advantage of the multidisciplinary expertise offered by the team conducting this review, the full-text analysis of the articles was divided on a disciplinary basis and led by a researcher with expertise relating to the subject matter discussed within the literature. For example, the Law Research Associate assessed papers with a legal focus, and Computing Science Research Associates assessed papers with a computer science focus.

To achieve this, we labelled the category of each paper based on the scope of the journal/conference where it is published. The category labels were Information Security, Human-Computer Interaction, Social Science, and Law. The papers in each category are sorted by reviewing priorities. Generally, the most recent papers published in top journals/conferences were prioritised and reviewed first. This decision was made considering the time limitation and ecological distribution of labour.

The data extracted included:

1. Articles that explore discussions about smart home vulnerabilities.
2. Articles that engage with themes of risks and harms in a smart home context.
3. Multidisciplinary studies and cross-comparative country case studies.

The abstracted data on article characteristics were aims/purpose, methods, research participant demographics, how outcomes were measured, research object (e.g., smart speaker, smart meter, user attitudes and perceptions), key contributions, opportunities for future research, representations of vulnerabilities, risks, and harms. Data on the country of the study was also abstracted based on information provided on research participant nationalities, country of policy, or country origin of smart home company/industry. However, this was only appropriate for social sciences, law, and some Human-Computer Interaction (HCI) studies and was not a meaningful category for information security as this information was often not included. As such, this characteristic was not utilised for the scoping review analysis. The objective of the rigorous procedure followed in this study was to ensure that the potential outcome synthesised the unidentified vulnerabilities, risks, and harms in the smart home context in order to understand how these complexities are construed, represented, and articulated in the literature.

We also address the Risk of Bias in Individual Studies. The internal peer review process is set to limit bias in the inclusion and exclusion of study selections. At least two of the initial reviewers independently assessed the risks of bias for each included article. A third or fourth reviewer from the data analysis team mediates in a conflict marked by Rayyan. To ensure reliability, we selected ten papers to be piloted before use to reach a consensus within the group regarding the selection criteria.

2.5. Stage 5 – collating, summarising, and reporting the results

Based on the selected papers, we analyse the results from three different perspectives:

1. *Quality of paper selection:* We utilise data science methods to estimate paper selection and labelling accuracy and quality. This ensures that screening and identifying relevant papers is conducted with precision.
2. *Interdisciplinarity and characteristics of the selected papers:* Through the application of data science and statistical methods, we present key numerical characteristics that reflect the multidisciplinary nature of the selected papers. This analysis provides insights into the agreement and distribution of papers across various research areas.
3. *Analysis of complex online harms:* We examine how risks, vulnerabilities, and harms are represented in different disciplines. By scrutinising the papers, we gain an understanding of the diverse perspectives and approaches to addressing these issues in the literature.

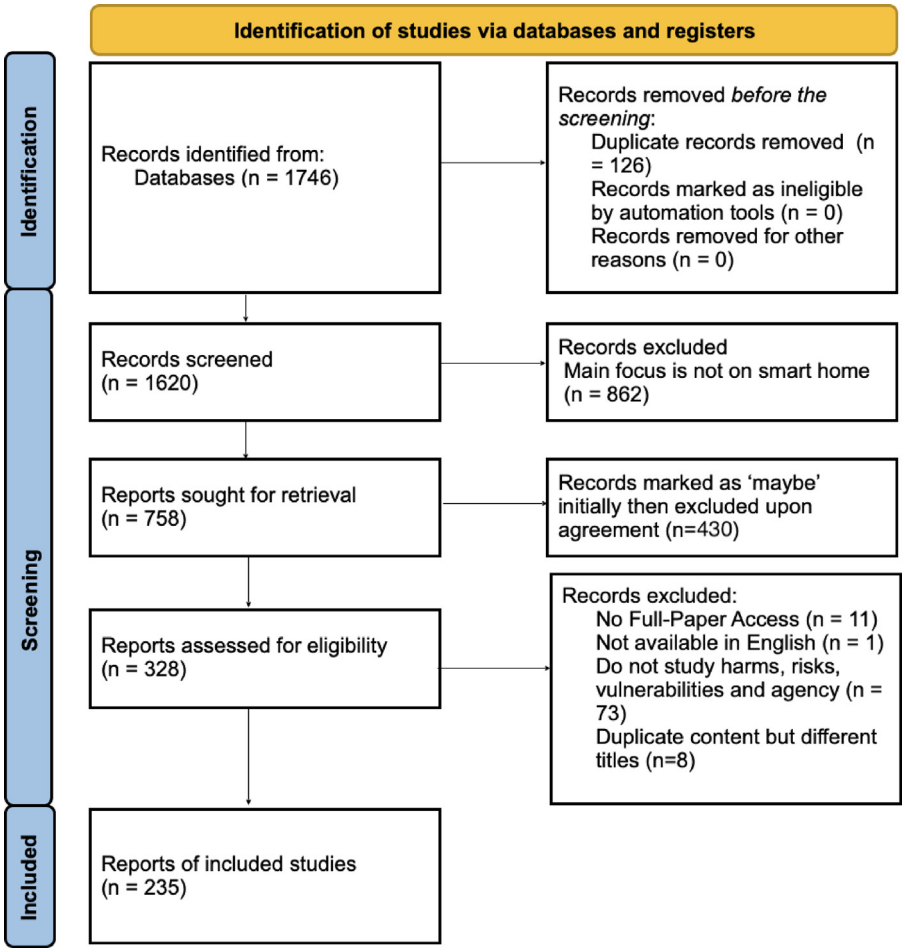


Fig. 1. Our process within this scoping review followed Arksey and O'Malley's five-stage methodological framework [26]. Additionally, the review followed the PRISMA Extension for Scoping Reviews (PRISMA-ScR) checklist (http://www.prisma-statement.org/Extensions/ScopingReviews) (accessed on 27 Feb 2023).

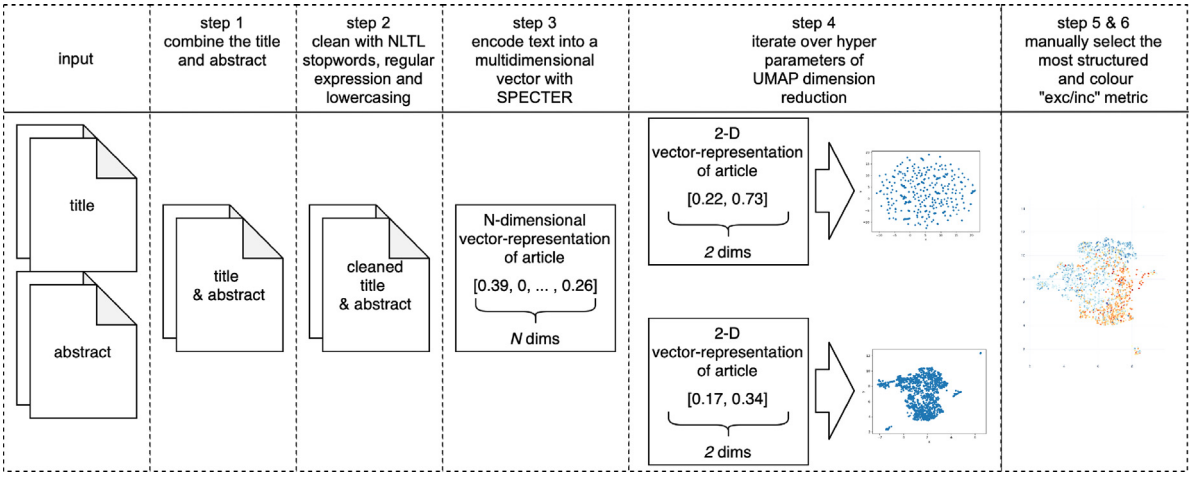


Fig. 2. Graphical representation of used pipeline for visualisation of articles inclusion/exclusion.

2.5.1. Quality of paper selection

To analyse the quality of the paper selection step, we utilised a Natural Language Processing technique to visualise text embeddings. The concept of this technique is that the researched articles can be plotted in a 2D scatterplot using a neural network, so the distance between each pair of articles reflects their difference. In this plot, more distant articles have different topics, while closer articles are more similar.

The technique included several steps depicted in Fig. 2:

1. For each article, we combined the title and abstract into a single string. We used these strings as input for the visualisation technique.
2. For each string, we clean the text by removing stopwords that were taken from the NTLK [31] stopwords list for the English language (removing common words like *'the'* or

'and'), removing punctuation and non-alphanumeric symbols with regular expressions and converting the text to lowercase.

3. Each string is encoded into a vector using the HuggingFace implementation [32] of the Specter [33] document-encoder model. We used an untuned version of the Specter model as it is already trained on scientific publications.
4. For the resulting vectors, we used UMAP [34] dimension reduction to reduce the multidimensional vector space into a 2D space that is suitable for the scatterplot. In this step, we also iterate over UMAP hyperparameters in the range [2:20] for the *n_neighbors* hyperparameter, and set {0.0001, 0.01, 0.1} for the *min_dist* hyperparameter while leaving other hyperparameters with default values. We save the resulting scatterplot for each iteration and manually select a scatterplot with a more visually structured representation.
5. Each paper is assigned an "exc/inc" metric, which is calculated by subtracting the number of votes "to exclude" from the number of votes "to include" the paper in the analysis (see stage 4).
6. The results are plotted with Plotly [35] in a scatterplot where each paper corresponds to a dot. The X and Y axes represent a 2D projection of the multidimensional space according to a UMAP algorithm and SPECTER encoder, respectively. The colour of each dot represents the "exc/inc" metric – the number of votes "to include" minus the number of votes "to exclude" from the analysis.

2.5.2. Interdisciplinarity and characteristics of the selected papers

For each included paper, we assigned a research area to answer the research questions from the perspective of each research direction (results of individual sources of evidence according to PRISMA). To do that, we compare the abstracts and titles of the papers with the research areas of the participating RAs in stage 4.

To summarise these data (synthesis of results according to PRISMA), we calculated the statistics of studies included in the review and depicted them in charts.

We also used two data science methods to estimate multidisciplinarity.

The first method measures the number of the same papers for each pair of research areas (security, HCI, social and law studies). Formally, we define an intersection as a cardinality of a set of papers $|S|$, such as $S = R_1 \cap R_2$, where the R_* is one of the defined research areas.

The second method is based on the distances between papers in sets. To find the closeness of the two disciplines, we used the following algorithm:

1. We used the papers' vector-space generated earlier through HuggingFace Specter (see embedding projection in Fig. 5 in the *results* section) to calculate the cosine distance $d_i = cosine(p_i, p_j)$ for each pair of papers, where first paper p_i is the paper from one research area such as $p_i \in R_1$, while the second paper is from another area $p_j \in R_2$ and is the nearest to the first paper $p_j = nearest(p_i, R_2)$.
2. We calculated the distance between areas d_{R_1,R_2} as an average of d_i such as $d_{R_1,R_2} = \frac{\sum_1^{|R_1|} d_i}{|R_1|}$.
3. As the numbers of papers in different research areas are not the same, their distances are not symmetric, $!\forall |R_1| = |R_2| \Rightarrow !\forall d_{R_1,R_2} = d_{R_2,R_1}$. Therefore, to make it symmetric, we took an average one again as $d_{R_1/R_2} = \frac{d_{R_1,R_2} + d_{R_2,R_1}}{2}$, so $\forall d_{R_1/R_2} = d_{R_2/R_1}$.

Table 1
Research areas of participated RAs.

Research area	Researcher
Information Security	MK, HW
Human-Computer Interaction (HCI)	SM (focus on voice assistants), VNZ
Social Sciences	SO, KM, JCA (focus on business studies)
Law	RO

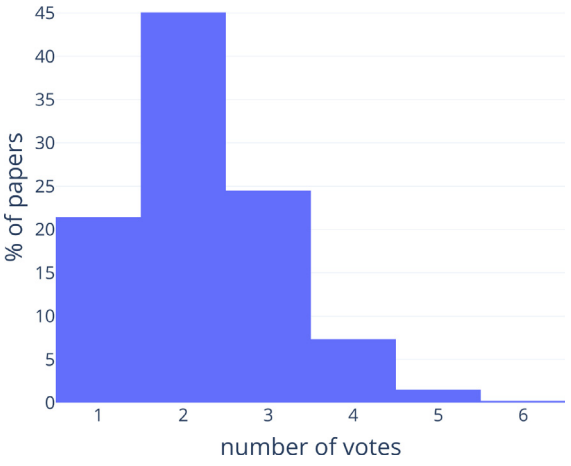


Fig. 3. Distribution of votes.

4. After this, we created a *MinMax* scale to calculate distances between areas and reverse them so that they can express similarity instead of dissimilarity $s_{R_1/R_2} = 1 - MinMax(d_{R_2/R_1}, D)$, $d_{R_2/R_1} \in D$.

These methodologies allowed us to gain insights into the multidisciplinary nature of the research areas and provide a comprehensive understanding of the relationships between them.

2.5.3. Complex online harms: Representations of risks, vulnerabilities, harms in different disciplines

The last methodology involves a manual analysis of selected papers obtained in stage 4, and is aimed at estimating how risks, vulnerabilities, and harms are represented across various disciplines. Through this analysis, we examine the themes associated with complex online harms, specifically focusing on risks, vulnerabilities, and harms within the fields of information security, human–computer interaction, social sciences, and law. It is discussed discipline-wise in more detail in Section 3.3

3. Results

A total of 8 research associates (RA) participated in the paper screening and identification (stages 1–4). The research areas of participants are presented in Table 1.

3.1. Quality of paper selection

After identifying relevant studies (stage 2), there were 1750 papers, while in stage 3, just 235 were included in the review. The result of each step of stage 3 is depicted in Fig. 1. These papers and 'inclusion' and 'exclusion' decisions are used as input data to estimate the quality of paper selection (see methodology presented in Section 2.5.1).

The distributions of the number of votes and "exc/inc" metric are presented in Figs. 3 and 4, respectively.

The final scatterplot, which indicates the similarity between papers, is shown in Fig. 5.

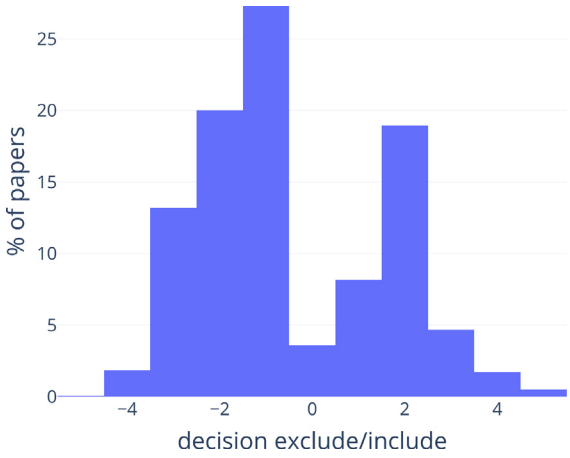


Fig. 4. Distribution of "exc/inc" metric.

One can notice on it that included papers have "exc/inc" metric > 0 and form a red pattern. The presence of a pattern in our selection indicates agreement between participated annotators and suggests that selected papers are not evenly distributed. Therefore, this means that this area corresponds to articles related to the vulnerabilities, risks, and harms of smart homes, and we can use them in Stage 5 in further research.

3.2. Interdisciplinarity and characteristics of the selected papers

The resulting set of papers (after stage 4) can be described with the following characteristics (characteristics of sources of evidence according to PRISMA ScR Reporting Guidelines):

1. Years published: in the range [2017-2022]
2. Language: English
3. Paper availability: full access version is available
4. Paper relevance: the relevance of the paper's content with the scoping review topic

We calculated the statistics of studies included in the review to summarise these data (synthesis of results according to PRISMA). We depicted it in Fig. 6 with Plotly [35]. The left side is the area chart of papers distribution over the year and research direction - the height of the whole area represents the total amount of papers, and the colour represents the fraction of a specific research direction. The right side is a pie chart of papers per research area. Each article was associated with one or multiple scientific areas: Security, Human-Computer Interaction, Social Sciences, and Law. Note that the total number of articles on the pie chart is more than 235 since scientific fields can overlap as some papers are interdisciplinary.

As one can see, most of the papers belong to Information Security. This is followed by HCI and Social Sciences, with just a few articles considering the Law.

A critical moment is that this plot does not explain how research areas intersect in the selected studies. Thus, we used two methods presented in Section 2.5.2 to measure the interdisciplinary of selected papers.

The result interdisciplinarity plots are depicted in Figs. 7 and 8, where columns and rows correspond to research areas and the cell to a number of same papers (Fig. 7) or similarity measure s (Fig. 8).

Figs. 7 and 8 indicates that the most significant gap between research areas is between information security and all other disciplinary areas. The highest similarity value gives the pair of social/law studies. Furthermore, for HCI, Social & Law are closer than information security.

3.3. Complex online harms: Representations of risks, vulnerabilities, harms in different disciplines

This scoping review identified emerging themes of 'risks', 'vulnerabilities', and 'harms' in that order of frequency for research on smart homes. It is worth noting that the frequency of terms used would be skewed towards computing science and information security literature as that comprised most of the literature. Threats also emerged as a common term accompanying those risks, harms, and vulnerabilities in the literature. They can therefore be included as a keyword in future research on complex online harms.

This section proceeds with a discussion of the themes related to the complex online harms of risks, vulnerabilities, and harms by field of literature; information security, human–computer interaction, social sciences, and law.

3.3.1. Information security

From an information security perspective, harm, vulnerability, and risk are formalised using different standards. Researchers typically mention harm to confidentiality, integrity, availability,[3] and privacy. Vulnerabilities in smart home devices are often described using standards such as the Common Vulnerabilities and Exposures (CVE) [36], Common Weakness Enumeration (CWE) [37], and the OWASP IoT TOP 10 [38]. Some researchers define vulnerabilities using the STRIDE model [39] and CAPEC [40], which focus on common attack vectors and patterns.

To describe risks, most researchers use the Common Vulnerability Scoring System (CVSS) [41] to prioritise defence mechanisms and the DREAD [42] model to analyse and evaluate risks.

Smart homes are typically analysed on three levels: (1) smart home devices and their components, (2) the smart home network, and (3) security protocols.

Research on smart home security focuses on developing novel approaches to detect and prevent information attacks specific to IoT environments. This includes developing firewalls, access control and authentication systems, and intrusion detection and prevention systems. Additionally, researchers work on developing novel risk analysis techniques to prioritise defence mechanisms and increase user awareness. Standardisation and review of existing vulnerabilities and trends are also important research areas.

The common limitation of the found research is the lack of support of their results by the 'real life experiments' and incident reports provided by commercial security companies.

In summary, frameworks like the CIA triad, vulnerability standards like CVE and CWE, and risk assessment models like CVSS and DREAD help researchers and practitioners identify and address weaknesses in smart home devices and networks. Developing new approaches for detecting and preventing attacks, risk analysis techniques, and standardisation and review of vulnerabilities are key research areas.

3.3.2. Human-computer interaction

From the Human-Computer Interaction (HCI) perspective, understanding the behaviours, perceptions, and attitudes of related stakeholders such as end users, gatekeepers, and entrepreneurs on smart home devices has been a necessary activity before identifying potential design solutions to the end users' concerns (e.g., [43,44]). Qualitative research methods such as surveys, interviews, focus groups, as well as other user-centred co-design methods employed by engaging with target users directly, are commonly adopted to engage with the target population closely (e.g., [44–50]). Across the scope of the research examined, HCI

[3] a.k.a. CIA triad.

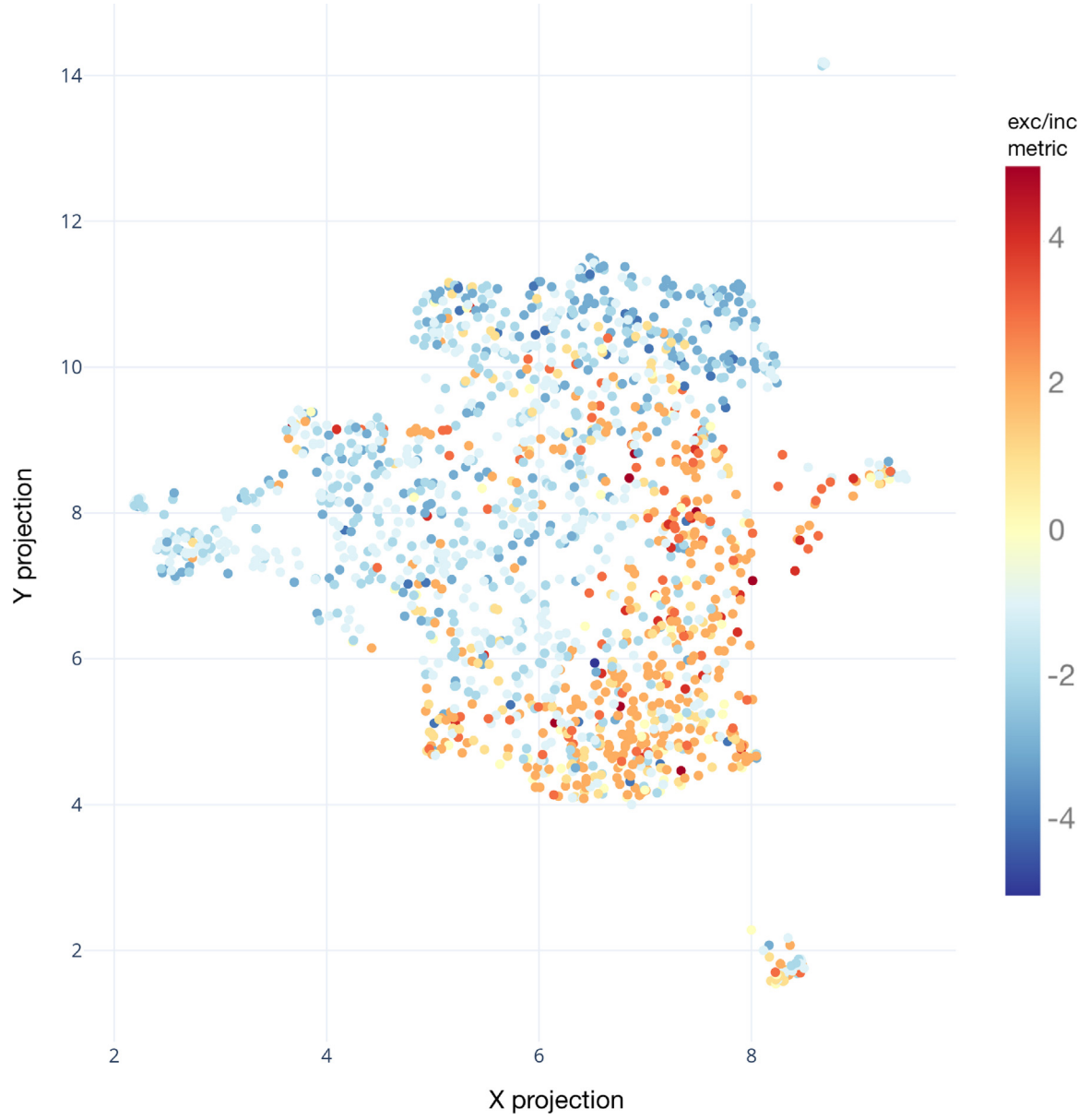


Fig. 5. Each paper is a dot with its colour indicating the "exc/inc" metric, and the X and Y are abstract projections of multidimensional axes indicating the similarity between papers.

researchers obtained an understanding of the users' experience (e.g.,[51–53]), attitudes of smart home devices towards everyday use and engagement with smart home devices, (e.g., [54,55]), explored and evaluated design ideations to promote an effortless user-centred digital household (e.g., [50]), or depicted and assessed the internal threats brought by smart home devices and how it may affect different users (e.g., [47,49]).

The specificity of such a focus unveiled the vulnerabilities, harms, and risks that users experience. Vulnerability is a key component for HCI designers to consider when defining research questions and allocating target groups when identifying and evaluating risks and harms, as well as leveraging agency in the smart home context (e.g., [56]). We highlighted two categories of 'vulnerabilities': the first indicates the users who are potentially vulnerable to malicious technologies (e.g., [57,58]); the second refers to the identified security issues existing in the Internet of Things (IoT) with or without a patch (e.g., [17,59]). In the first perspective, existing literature has specifically explored population groups, including older people, individuals with disabilities, and children (e.g., [57,58,60]). Other related literature identified whoever may be influenced by risks and harms in the smart home context as 'vulnerabilities' (e.g., [17,59]). Existing research has also proposed various design implications and policy considerations regarding how much information should be controlled by and shared with users that can benefit both the development of smart home technologies and the privacy concerns of end users (e.g., [61]). Power dynamics within the digital household, which led to an investigation of vulnerable groups have been given arising attention (e.g., [47,58]). Risk assessment models, safety messaging systems, authentication mechanisms, AR-based interaction systems, and new speaker and robot designs have been deployed, tested, and analysed to protect people against cybersecurity infringement within the smart home ecosystem (e.g., [62,63]). Existing empirical work shares similar limitations, including limited sample size, short observation time, and simplified survey instruments (e.g., [64]). In addition, more vulnerabilities call for attention, such as the population who may experience social isolation and marginalisation. A broader scenario within the IoT

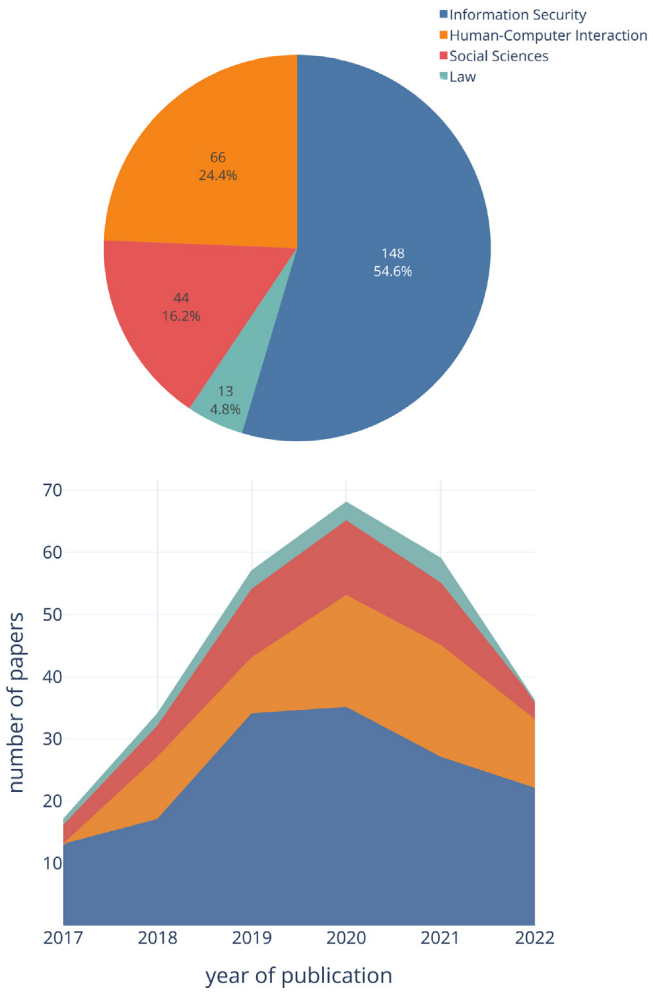


Fig. 6. Distributions of selected paper per year and research area.

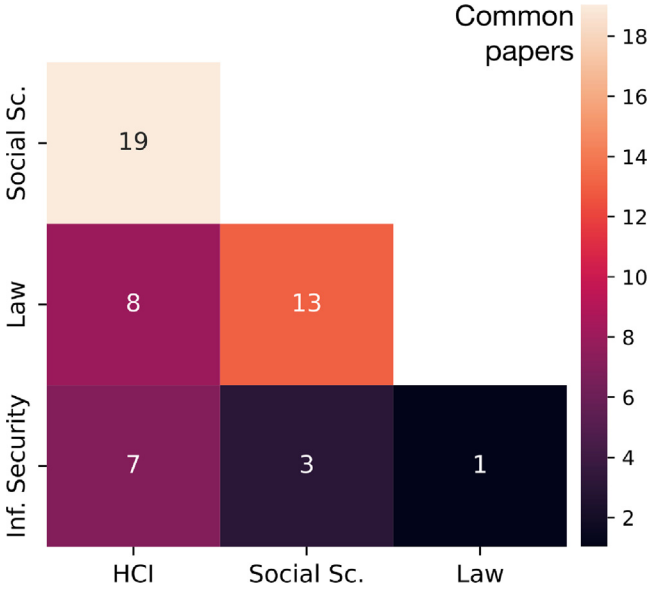


Fig. 7. Research areas similarity based on method 1 (similarity based on set cardinality – each number in the matrix is a number of same papers for each pair of research areas).

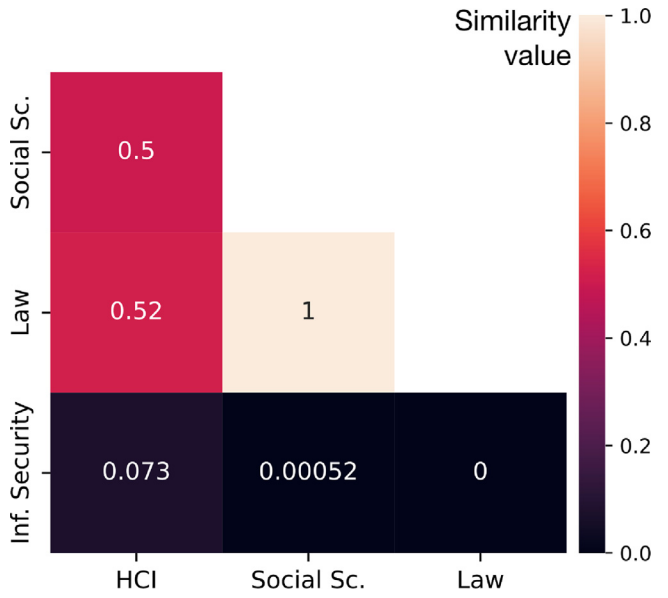


Fig. 8. Research areas similarity based on method 2 (similarity based on distances between papers encoded with NLP methods and SPECTER model in sets – each number in the matrix is a *MinMax* normalised and reversed cosine distance).

environment, a more diverse inclusion of technologies, and a higher level of ethical principles must be situated, adopted, and operationalised in future work.

Several themes emerged across the literature that broadly revolve around concepts of agency and autonomy. For one, the literature highlights privacy and cyber security issue as key risks and vulnerabilities in smart home systems, delimiting the user's experience but also as perceived causes of direct and indirect harm.

Correspondingly, the lack of awareness, knowledge, and perhaps digital literacy more broadly escalates the problem of vulnerabilities, risks, and harms encountered in smart home contexts. [65] noted that cybersecurity exploitation mostly occurs without the victim's knowledge of the scenario. This has been explicitly demonstrated in cyber-abuse cases involving domestic violence. [55] states that smart home environments are affected by knowledge, awareness, trust, and risk tolerance. These digital literacy gaps reinforce offline inequalities. For instance, in cyber abuse cases, coercive control deployed within smart systems largely reflects the gaps in the digital literacy of users. Research shows that smart home users do not pay keen attention to perceived privacy risks when providing privacy data for a better bespoke service in smart home contexts [66]. From a user perspective, the research shows that users generally cede their agency, independence, and autonomy in the smart home in favour of increased benefits of technology, which then augments risks and vulnerabilities. More so, smart home users are depicted as generally 'unaware of privacy risks from inference algorithms operating on data from non-audio/visual devices' [67].

The use of digital voice assistants has grown rapidly in the last decade. It is forecasted that, by 2024, the number of digital voice assistants will reach 8.4 billion units – a number higher than the world's population.[4] A similar trend is followed in the field of Smart Home Personal Assistants (SPA). But the users are concerned about these devices' security and privacy [68,69] as they mostly rely on the voice communication channel, which is known to be vulnerable, lacking proper authentication. Despite

[4] https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/

the fast-growing research on SPA's security and privacy issues, the literature lacks a detailed characterisation. We observed that while security and privacy attacks over SPA are distinctly broad, the researchers have focused only on a smart part of it. Notably, the recent works are mostly related to the issues of direct interaction between a user, and their SPA [70–72]. However, those problems are indeed important and require further research to find effective countermeasures. Further attention should also be paid to issues related to authorisation, speech recognition, profiling, and the technologies integrated with SPA (e.g., the cloud, third-party skills, and other smart devices).

The evidence suggests that the SPA research community requires robust methods for practical evaluation of existing attacks and countermeasures [72,73]. We noted that the interaction between the users and the SPA devices needs to be improved. SPA with *always on, always listening features* is more vulnerable if they do not have robust authentication criteria [74]. Currently, the authentication mechanisms in smart homes are mostly decentralised. Incorporating a centralised mechanism would enable a user to access multiple integrated technologies by lessening the authentication burden and improving security measures. However, this must be implemented carefully to avoid creating a single point of failure. Hence, future research focuses on how communication protocols may improve current authentication mechanisms in SPA.

The next challenge of personal assistants in smart homes is to control and manage authorisation, as the literature suggests that the authorisation mechanism should be able to dynamically authorise and adapt permissions to users based on the current context and their preferences [75,76]. It is shown that SPA requires a more fine-grained authorisation mechanism. We observe no formal security and privacy mechanisms for SPA that consider *multi-user environment issues* [77]. The lack of proper authorisation measures can cause insider misuse or lead to legal issues, e.g. intimate partner abuse. Moreover, the smart home itself refers to a group of technologies collectively. Future research requires novel authorisation mechanisms that provide secure access authorisation and allow users to specify, monitor and control what data can be shared with those that have no direct access to the SPA architecture, under what conditions and for what purpose.

SPA is involved with many Natural Language Processing (NLP) and Machine Learning (ML) for speech recognition to sound more natural and realistic [78,79]. Manipulation in these models can again cause severe security and privacy issues [80]. To handle this, SPA providers must check for adversarial examples with robust AI-based countermeasures. In addition, most existing SPAs processes users' voices in the cloud, making it difficult again to ensure privacy issues [81,82]. Therefore, there is a need for future efforts on how to make voice processing privacy-preserving without hindering SPA's capabilities effectively. Future work should also look at the best, and most systematic way to conduct privacy assessments in SPA [83].

The investigations relating to smart home devices with the broader literature in the HCI broadly employ qualitative methods and principally conduct interviews, focus group discussions, and participatory approaches. Across the scope of the research examined, two dynamics are examined in the literature: one refers to the experience [51–53] and attitudes of smart home users towards everyday use and engagement with smart home devices, and the other to their perception of such devices [54,55]. The specificity of such a focus helps us to unveil the vulnerabilities, harms, and risks that users experience from a user-centred perspective.

3.3.3. Social sciences

The taxonomy of the vulnerabilities, risks, and harms relevant to smart home contexts are increasingly becoming established, with complexities in the security and privacy architecture of such devices being the focal point of debate, digital literacy, knowledge gaps and awareness, adversarial and malicious attacks and surveillance and control. Accompanying corresponding risks to users are imbalances in understanding how these ills operate, therefore, in understanding the scope and scale of the problem. Cyber security, privacy, and literacy escalate legal concerns, access and social exclusion issues, inequality, performance, abuse, and data breaches within smart homes and require further research. In the United Kingdom, with increasingly developing attention to cyber abuse and deficits in agency and autonomy of users within the home context.

Much of the smart-home literature in the domain of social sciences focused on enhancing understanding of the perceived benefits and risks surrounding and influencing acceptance and adoption of smart-home systems from the perspectives of prospective and current users, industry and policymakers to identify the discrepancies among these multi-stakeholders [4]. The research aims to provide insight into dismantling barriers to support and further shape the market development and adoption of smart-home technologies. For this purpose, many studies employed surveys to conduct statistical analysis generating the results which, in contribution to the field, are then (captured and) built into a conceptual framework to determine and hence advance the understanding of the motivating and demotivating factors to use smart-home systems. Much of this work constructs a conceptual framework by combining the key elements of the extant theories. For instance, [84] incorporate constructs from the Technology Acceptance Model (TAM), which predicts and explains users' acceptance of technology, the Innovation Diffusion Theory (IDT), which explains the diffusion of the innovation process, passing from innovation development to shaping the user attitudes and then to the final decision whether to adopt or reject, and the Perceived Risk Theory (PRT) postulated to impact the user adoption decision of technical innovations.

In contrast, Mulcahy et al. [85] draw from a different set of the major frameworks and concepts in the literature, namely, the Technology Readiness Index (TRI). This examines whether consumers wish to engage, the Consumer Engagement, which shows how consumers see themselves engaging, and Trust and Risk, which examine factors motivating or demotivating for adoption and engagement. Whilst relying on a systematic literature review of smart-home technologies, Li et al. [86] also develop a conceptual framework to understand the motivations, barriers, and risks associated with the choice to adopt smart-home systems from a consumer perspective.

Within the business studies literature, a socio-technological perspective was taken in relation to smart homes, where users were often viewed from the standpoint of consumers and users of smart home devices and IoT. As it relates to complex online harms, the term risk appeared the most frequently, followed by harm and vulnerability. Themes of risk were found to be linked to the commercial success of consumers adopting smart home devices and IoT [87], user anxiety and perceptions of risks around privacy and security such as the sharing of their data with third parties [88–90], and risks of smart homes exacerbating societal inequalities through furthering exclusion of already marginalised groups [23]. Similar to societal risks were the themes of incurring societal harm through social divides experienced by different demographics using smart home technology [91]. Harms to consumers were also considered, such as the manipulation of consumer behaviour, profiling, price discrimination, and targeted predatory advertising [92]. Other general harms were those of

threats to the security and privacy of smart home devices [93]. The term 'vulnerability' was found to take two different meanings. Firstly, it parallelled the findings for computing science and information security literature, where vulnerability was also used in business literature to refer to smart devices with poor cybersecurity [94]. Secondly, there was a socio-technical understanding of vulnerability, which meant user mis-perceptions and lack of knowledge around smart home technologies [95]. The participants in the studies conducted by the business literature spanned business use cases within the smart home industry [92], interviews with IoT experts, smart home designers, and persons working in the smart home industry [87,93], as well as surveys and focus groups of smart home customers [85,88,89,91].

Future research should establish a responsible digital innovation agenda to safeguard consumer privacy and establish a foundation of trust within the smart home industry [88].

3.3.4. Law

From a legal point of view, contemporary literature is extremely limited regarding the risks, harms, and vulnerabilities of smart homes. This scoping review identified 4.8% of papers matching our legal literature criteria.

Our analysis shows that, under a legal framework, harms are classified as situational or informational based on the risks posed by cybercrime activity or privacy and data concerns [96]. Much of the literature adopts a legal doctrinal approach to evaluate the regulation of smart home devices in terms of existing legal standards such as data protection law and the UK's Code of Practice for Consumer IoT Security [96–98]. An exception is the work of Chen and Urquhart [94], who employ a social-technical analysis of barriers to securing IoT devices. From a legal perspective, smart home users are assumed to lack agency resulting from information asymmetries between stakeholders controlling the device and a lack of technical capabilities [96,97]. This has led to calls to reassign legal responsibility and accountability to smart home device manufacturers to protect stakeholders adequately [94,97].

However, given the lack of literature in this area, it is clear that further research is needed to inform the legal understanding of the risk, harms and vulnerabilities of smart home devices and to explore ways in which policy can be utilised to support responsible smart home innovation.

4. Discussion

This section provides an overall assessment of the literature and discusses how it relates to the research questions. An overview of the limitations of this study and suggestions for future research follow this.

4.1. Assessment of literature

This work highlighted the existing literature on smart homes has had a heavy technology focus. This huge imbalance in the literature is also reflected in the dataset deployed in this work, where the balance between papers in the broad areas of humanities and social science is far fewer than those with a technical focus of computer science.

Regarding research question one (how are smart home harms/risks/vulnerabilities conceived, encountered, addressed, and tackled in the literature?), it was found that the computing science/information security general premise of vulnerability as poor cyber security of smart devices has infiltrated the social sciences understanding of vulnerability as well. However, social sciences literature approaches complex online harms from a socio-technical perspective by considering the impact on smart home users' perceptions and intention to adopt smart home technology and the societal consequences. The differences in the understandings and uses of the terms risks, vulnerabilities, and harms emphasise the importance of an all-encompassing concept, such as complex online harms, to foster insights through a collaboration of multidisciplinary perspectives. This finding indicates that to empower users in the smart home environment, perspectives of HCI and social sciences need to be included in cyber security designs of smart home technologies, and they also need to be phrased in ways that can be easily understood by any user [93].

In terms of the second research question, which investigated how digital agency is undermined and obtained in the smart home environment, the scoping review found that the literature did not explicitly address agency in the specific context of users and that themes surrounding agency tended to be implied, except for one paper, i.e.[11]. Therefore, at the moment, it is difficult to engage the concept of user agency within the smart home. However, considering digital social innovation, it is clear that user agency can serve as an evaluative tool for complex online harms. This paper previously outlined the above agency as the control and autonomy of digital citizens in the smart home [9,10]. Thus, a human-controlled 'agency re-adjustment' of autonomous and proactive smart home technologies is necessary to benefit users sustainably [11]. A scenario where human users' motives and needs cannot be prioritised when they expect the technologies to be a 'collaborator' and provide recommendations for decision-making may turn human users into 'vulnerables' and bring potential risks and harm to people [11].

Moreover, a scenario where smart home devices fail to take the role of 'executor' when human users expect the full conveniences also fails to engage with human users in the long term. The values, including efficiency, emotional bonding, and privacy, that end users appropriate for these technologies define the agency that smart home devices should possess. These values defining agency should form part of the reference criteria for driving the digital innovation of the market.

4.2. Limitations

This scoping review concentrated on the risks, harms, and vulnerabilities in the smart home context from a multidisciplinary approach. Therefore, some limitations to this review are worth noting. Firstly, the inherent nature of a scoping review itself decides the breadth rather than the depth of the review. As such, this study could not provide an in-depth analysis of how different demographics become empowered and disempowered during interactions with smart home technologies. However, this work fulfilled our objective of identifying and examining studies' key concepts and characteristics and the knowledge gaps across disciplines. In addition, we limited our work selection to published and written in English. This was a pragmatic decision based on accessibility and the need to standardise our approach. A further limitation is that our analysis is limited to papers published between 2017 and 2022, which may restrict the scope of our findings. However, given the capacity of IoT smart home devices for technological change, this decision to limit our findings to contemporary literature is justified.

4.3. Future research

This scoping review aimed to provide insights into the landscape of literature on complex online harms and smart homes. While this provided some summative context as to the different demographics that become empowered (e.g. affluent, educated) and, respectively, disempowered (e.g., elderly, lacking in digital literacy, societally marginalised) by smart home technologies [8,

23,91]. A systematic literature review is needed to understand how different user demographics may be empowered and disempowered by smart homes. Furthermore, policymakers have aimed to cultivate safe online experiences (e.g., the Online Safety Bill and The Code of Practice for Consumer IoT Security). This scoping review revealed a considerable disparity in legal academic interest in harm within the smart home compared with other disciplines. As a result, there is a clear need to undertake further conceptual and empirical research in this area. Future research could also be undertaken to engage with issues around the ethical use of smart homes. This could be achieved by employing innovative methodological approaches such as case studies that are largely absent from the literature, including multi-modal and participatory design approaches with a user-centric focus.

5. Conclusion

This study is a scoping review of emergent conceptualisations of risks, harms, and vulnerabilities in the literature on smart homes. The main strength of this paper lies in its interdisciplinary review and approach, which draws on a multidisciplinary lens, including human–computer interaction, information security, social sciences, and law. Resolving the human and social dimensions of technology design, adoption, and usage are implicit components of the intersection between human–computer interaction (HCI) and social science. Concerning the research questions and the developing literature, this review identified emerging themes of 'risks', 'vulnerabilities', and 'harms' in that order of frequency within the literature on smart homes. The usage of terms is skewed towards computing science and information security as that comprised the majority of the literature at 54.6%.

Regarding the second research question about how digital agency is undermined and obtained in the smart home environment, the literature brings up issues with privacy, monitoring, and consent as lapses in the design of smart home technologies. As a contribution, it is argued that human–computer interaction may draw from social science research by gaining knowledge about the societal effects of these technologies and the ethical considerations for design so they can develop technologies that respect user privacy, deal with power inequalities, and safeguard informed consent. The paucity of research in the social sciences indicates a need for research focusing on user-centred perspectives. Studies on user attitudes and behaviour can shape understanding of how users perceive and respond to the harms associated with the smart home, likewise the stimulus for adoption or refusal of smart home systems. In these areas, more studies are needed to bridge the literature gap and complement research in human–computer interaction. Social science and legal research can seek ways to empower users by giving them agency and more autonomy within the smart home ecosystem through policies and educational interfaces that provide insight to users about the scale and scope of harms, risks, and vulnerabilities and ways to mitigate them. As a result, further research is needed to develop a technology-conscious, citizen-centred approach to understanding and combating smart homes' risks, harms and vulnerabilities.

CRediT authorship contribution statement

Shola Olabode: Conceptualisation, Methodology, Software, Writing – original draft, Data curation, Document organisation. **Rebecca Owens:** Conceptualisation, Methodology, Software, Data curation, Writing – original draft. **Viana Nijia Zhang:** Conceptualisation, Methodology, Software, Writing – original draft, Data curation, Document organisation. **Jehana Copilah-Ali:** Conceptualisation, Methodology, Software, Writing – original draft, Data curation. **Maxim Kolomeets:** Software, Writing – original draft, Data curation, Data visualisation, Document organisation. **Han Wu:** Software, Data curation, Document organisation. **Shrikant Malviya:** Software, Writing – original draft, Data curation, Data visualisation. **Karolina Markeviciute:** Software, Data curation. **Tasos Spiliotopoulos:** Writing – reviewing. **Cristina Neesham:** Writing – reviewing. **Lei Shi:** Writing – reviewing. **Deborah Chambers:** Writing – reviewing, Supervisor.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Shola Olabode reports financial support was provided by Newcastle University and UK Research and Innovation (UKRI).

Data availability

No data was used for the research described in the article.

Acknowledgements

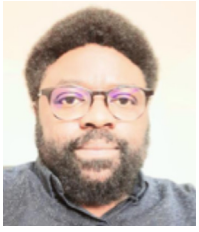
The authors of this paper are part of research supported by UK Research and Innovation, United Kingdom through the Strategic Priority Fund as part of the Protecting Citizens Online programme. Grant: *"AGENCY: Assuring Citizen Agency in a World with Complex Online Harms"*, EP/W032481/2 at Newcastle University, United Kingdom, Birmingham University, and Durham University, United Kingdom.

References

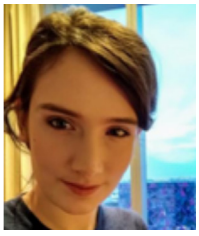
[1] M.E. Cho, M.J. Kim, Smart homes supporting the wellness of one or two-person households, Sensors 22 (20) (2022) 7816.
[2] R. Creaney, L. Reid, M. Currie, The contribution of healthcare smart homes to older peoples' wellbeing: A new conceptual framework, Wellbeing Space Soc. 2 (2021) 100031.
[3] D. Lupton, The internet of things: social dimensions, Sociol. Compass 14 (4) (2020) e12770.
[4] C. Wilson, T. Hargreaves, R. Hauxwell-Baldwin, Benefits and risks of smart home technologies, Energy Policy 103 (2017) 72–83.
[5] F.K. Aldrich, Smart homes: Past, present and future, in: Inside the Smart Home, Springer-Verlag, London, 2006, pp. 17–39.
[6] J. Shin, Y. Park, D. Lee, Who will be smart home users? An analysis of adoption and diffusion of smart homes, Technol. Forecast. Soc. Change 134 (2018) 246–253.
[7] I. Agrafiotis, J.R.C. Nurse, M. Goldsmith, S. Creese, D. Upton, A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, J. Cybersecur. 4 (1) (2018).
[8] B. Sovacool, D.F. Del Rio, S. Griffiths, Policy mixes for more sustainable smart home technologies, Environ. Res. Lett. 16 (5) (2021) 054073.
[9] A. Bandura, Social cognitive theory: an agentic perspective, Annu. Rev. Psychol. 52 (1) (2001) 1–26.
[10] N. Cila, I. Smit, E. Giaccardi, B. Kröse, Products as agents: Metaphors for designing the products of the IoT age, in: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17, Association for Computing Machinery, New York, NY, USA, 2017, pp. 448–459, http://dx.doi.org/10.1145/3025453.3025797.
[11] R. Garg, H. Cui, Social contexts, agency, and conflicts: Exploring critical aspects of design for future smart home technologies, ACM Trans. Comput.-Hum. Interact. 29 (2) (2022) 1–30.
[12] M. Tabassum, T. Kosinski, H.R. Lipford, I don't own the data: End user perceptions of smart home device data practices and risks, in: SOUPS @ USENIX Security Symposium, 2019.
[13] J. Westheimer, J. Kahne, What kind of citizen? The politics of educating for democracy, Am. Educ. Res. J. 41 (2) (2004) 237–269.
[14] D. Byrne, Complexity Theory and the Social Sciences: An Introduction, Routledge, 2002.
[15] M. Reed, D.L. Harvey, The new science and the old: Complexity and realism in the social sciences, J. Theory Soc. Behav. 22 (4) (1992) 353–380.

[16] Y.Y. Haimes, On the definition of resilience in systems, Risk Anal. 29 (4) (2009) 498–501.
[17] L. Costa, J.P. Barros, M. Tavares, Vulnerabilities in IoT devices for smart home environment, in: Proceedings of the 5th International Conference on Information Systems Security e Privacy, ICISSP 2019, Vol. 1, SciTePress, 2019, pp. 615–622.
[18] Ofcom, Internet users' online experiences and attitudes qualitative research summary, 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0022/157153/online-experiences-attitudes-qualitative-summary-report.pdf, (Accessed on 20.02.2023).
[19] R. Jamwal, H.K. Jarman, E. Roseingrave, J. Douglas, D. Winkler, Smart home and communication technology for people with disability: a scoping review, Disability Rehabil.: Assistive Technol. 17 (6) (2022) 624–644.
[20] Z. Munn, M.D.J. Peters, C. Stern, C. Tufanaru, A. McArthur, E. Aromataris, Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach, BMC Med. Res. Methodol. 18 (1) (2018) 143.
[21] X. Wang, T.J. McGill, J.E. Klobas, I want it anyway: Consumer perceptions of smart home devices, J. Comput. Inf. Syst. 60 (5) (2020) 437–447.
[22] H.L. Colquhoun, D. Levac, K.K. O'Brien, S. Straus, A.C. Tricco, L. Perrier, M. Kastner, D. Moher, Scoping reviews: time for clarity in definition, methods, and reporting, J. Clin. Epidemiol. 67 (12) (2014) 1291–1294.
[23] Layton, Steel, The convergence and mainstreaming of integrated home technologies for people with disability, Societies (Basel) 9 (4) (2019) 69.
[24] D. Marikyan, S. Papagiannidis, E. Alamanos, The effect of behavioural beliefs on smart home technology adoption, in: UK Academy for Information Systems Conference Proceedings, 2019.
[25] A.C. Tricco, E. Lillie, W. Zarin, K.K. O'Brien, H. Colquhoun, D. Levac, D. Moher, M.D.J. Peters, T. Horsley, L. Weeks, S. Hempel, E.A. Akl, C. Chang, J. McGowan, L. Stewart, L. Hartling, A. Aldcroft, M.G. Wilson, C. Garritty, S. Lewin, C.M. Godfrey, M.T. Macdonald, E.V. Langlois, K. Soares-Weiser, J. Moriarty, T. Clifford, Ö. Tunçalp, S.E. Straus, PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation, Ann. Intern. Med. 169 (7) (2018) 467–473.
[26] H. Arksey, L. O'Malley, Scoping studies: towards a methodological framework, Int. J. Soc. Res. Methodol. 8 (1) (2005) 19–32.
[27] M.D.J. Peters, C. Marnie, A.C. Tricco, D. Pollock, Z. Munn, L. Alexander, P. McInerney, C.M. Godfrey, H. Khalil, Updated methodological guidance for the conduct of scoping reviews, JBI Evid. Synth. 18 (10) (2020) 2119–2126.
[28] D. Archibald, R. Patterson, E. Haraldsdottir, M. Hazelwood, S. Fife, S.A. Murray, Mapping the progress and impacts of public health approaches to palliative care: a scoping review protocol, BMJ Open 6 (7) (2016) e012058.
[29] A.M. Methley, S. Campbell, C. Chew-Graham, R. McNally, S. Cheraghi-Sohi, PICO, PICOS and SPIDER: a comparison study of specificity and sensitivity in three search tools for qualitative systematic reviews, BMC Health Serv. Res. 14 (1) (2014) 579.
[30] M. Ouzzani, H. Hammady, Z. Fedorowicz, A. Elmagarmid, Rayyan—a web and mobile app for systematic reviews, Systematic Rev. 5 (2016) 1–10.
[31] E. Loper, S. Bird, Nltk: The natural language toolkit, 2002, arXiv preprint cs/0205028.
[32] Allen Institute for A.I., HuggingFace specter model, 2022, https://huggingface.co/allenai/specter, (Accessed on 27.02.2023).
[33] A. Cohan, S. Feldman, I. Beltagy, D. Downey, D.S. Weld, Specter: Document-level representation learning using citation-informed transformers, 2020, arXiv preprint arXiv:2004.07180.
[34] L. McInnes, J. Healy, J. Melville, Umap: Uniform manifold approximation and projection for dimension reduction, 2018, arXiv preprint arXiv:1802.03426.
[35] Plotly Technologies Inc, Plotly chart studio, 2023, https://plotly.com/, (Accessed on 27.02.2023).
[36] MITRE, Common vulnerabilities and exposures (CVE), 2023, https://cve.mitre.org/, (Accessed on 27.02.2023).
[37] MITRE, Common weakness enumeration (CWE), 2023, https://cwe.mitre.org/, (Accessed on 27.02.2023).
[38] OWASP, Top 10, 2021, https://owasp.org/www-project-top-ten/, (Accessed on 27.02.2023).
[39] Microsoft, STRIDE, 2009, https://www.microsoft.com/en-us/security/blog/2009/08/27/the-threats-to-our-products/, (Accessed on 27.02.2023).
[40] MITRE, Common attack pattern enumerations and classifications (CAPEC), 2023, https://capec.mitre.org/, (Accessed on 27.02.2023).
[41] FIRST, Common vulnerability scoring system (CVSS), 2023, https://www.first.org/cvss/, (Accessed on 27.02.2023).
[42] A. Shostack, Experiences threat modeling at microsoft, in: MODSEC@MoDELS, 2008, p. 35.
[43] A. Förster, J. Block, User adoption of smart home systems, in: Proceedings of the 2022 ACM Conference on Information Technology for Social Good, GoodIT '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 360–365, http://dx.doi.org/10.1145/3524458.3547118.
[44] E.-S. Katterfeldt, N. Dittert, Co-designing smart home maker workshops with girls, in: Proceedings of the Conference on Creativity and Making in Education, in: FabLearn Europe'18, Association for Computing Machinery, New York, NY, USA, 2018, pp. 100–101, http://dx.doi.org/10.1145/3213818.3213833.
[45] S. Rus, S. Helfmann, F. Kirchbuchner, A. Kuijper, Designing smart home controls for elderly, in: Proceedings of the 13th ACM International Conference on PErvasive Technologies Related to Assistive Environments, PETRA '20, Association for Computing Machinery, New York, NY, USA, 2020, http://dx.doi.org/10.1145/3389189.3392610.
[46] R. Abdallah, L. Xu, W. Shi, Lessons and experiences of a DIY smart home, in: Proceedings of the Workshop on Smart Internet of Things, SmartIoT '17, Association for Computing Machinery, New York, NY, USA, 2017, http://dx.doi.org/10.1145/3132479.3132488.
[47] Y. Strengers, J. Kennedy, P. Arcari, L. Nicholls, M. Gregg, Protection, productivity and pleasure in the smart home: Emerging expectations and gendered insights from Australian early adopters, CHI '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 1–13, http://dx.doi.org/10.1145/3290605.3300875.
[48] R.H. Jensen, Y. Strengers, D. Raptis, L. Nicholls, J. Kjeldskov, M.B. Skov, Exploring hygge as a desirable design vision for the sustainable smart home, in: Proceedings of the 2018 Designing Interactive Systems Conference, DIS '18, Association for Computing Machinery, New York, NY, USA, 2018, pp. 355–360, http://dx.doi.org/10.1145/3196709.3196804.
[49] J. Pierce, C. Weizenegger, P. Nandi, I. Agarwal, G. Gram, J. Hurrle, H. Liao, B. Lo, A. Park, A. Phan, M. Shumskiy, G. Sturlaugson, Addressing adjacent actor privacy: Designing for bystanders, co-users, and surveilled subjects of smart home cameras, in: Designing Interactive Systems Conference, DIS '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 26–40, http://dx.doi.org/10.1145/3532106.3535195.
[50] R. Garg, H. Cui, Social contexts, agency, and conflicts: Exploring critical aspects of design for future smart home technologies, ACM Trans. Comput.-Hum. Interact. 29 (2) (2022) http://dx.doi.org/10.1145/3485058.
[51] A. Alshehri, M.B. Salem, L. Ding, Are smart home devices abandoning IPV victims? in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, 2020, pp. 1368–1375.
[52] L.K. Aagaard, When smart technologies enter household practices: The gendered implications of digital housekeeping, Hous. Theory Soc. (2022) 1–18.
[53] L. Reid, Home as riskscape: Exploring technology enabled care, Geogr. J. 187 (2) (2021) 85–97.
[54] S. Zheng, N. Apthorpe, M. Chetty, N. Feamster, User perceptions of smart home IoT privacy, Proc. ACM Hum.-Comput. Interact. 2 (CSCW) (2018) http://dx.doi.org/10.1145/3274469.
[55] B. Sovacool, D.F. Del Rio, S. Griffiths, Policy mixes for more sustainable smart home technologies, Environ. Res. Lett. 16 (5) (2021) 054073.
[56] P.-D. Jarvis, A. Damianou, C. Ciobanu, V. Katos, Vulnerability exposure driven intelligence in smart, circular cities, Digit. Threats 3 (4) (2022) http://dx.doi.org/10.1145/3487059.
[57] R. Latikka, R. Rubio-Hernández, E.S. Lohan, J. Rantala, F. Nieto Fernández, A. Laitinen, A. Oksanen, Older adults' loneliness, social isolation, and physical information and communication technology in the era of ambient assisted living: A systematic literature review, J. Med. Internet Res. 23 (12) (2021) e28022.
[58] K. Sun, Y. Zou, J. Radesky, C. Brooks, F. Schaub, Child safety in the smart home: Parents' perceptions, needs, and mitigation strategies, Proc. ACM Hum.-Comput. Interact. 5 (CSCW2) (2021) http://dx.doi.org/10.1145/3479858.
[59] H. Liu, T. Spink, P. Patras, Uncovering security vulnerabilities in the belkin WeMo home automation ecosystem, in: 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019, pp. 894–899, http://dx.doi.org/10.1109/PERCOMW.2019.8730685.
[60] D. Brand, F.D. DiGennaro Reed, M.D. Morley, T.G. Erath, M.D. Novak, A survey assessing privacy concerns of smart-home services provided to individuals with disabilities, Behav. Anal. Pract. 13 (1) (2020) 11–21.
[61] H. Wang, T. Feng, Z. Ren, L. Gao, J. Zheng, Towards efficient privacy-preserving personal information in user daily life, in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer International Publishing, Cham, 2020, pp. 503–513.
[62] J.-P. Lee, S.-H. Lee, J.-G. Lee, J.-K. Lee, Design of device mutual authentication protocol in smart home environment, in: Computational Science/Intelligence & Applied Informatics, in: Studies in computational intelligence, Springer International Publishing, Cham, 2019, pp. 135–148.
[63] C. Haidon, H. Pigot, S. Giroux, Joining semantic and augmented reality to design smart homes for assistance, J. Rehabil. Assist. Technol. Eng. 7 (2020) 2055668320964121.

[64] B. Taieb, J.-É. Pelet, The user's attitude and security of personal information depending on the category of IoT, in: Advances in Intelligent Systems and Computing, Springer International Publishing, Cham, 2019, pp. 431–437.
[65] F. James, A risk management framework and a generalized attack automata for IoT based smart home environment, in: 2019 3rd Cyber Security in Networking Conference (CSNet), IEEE, 2019, pp. 86–90.
[66] D.F. Del Rio, Smart but unfriendly: Connected home products as enablers of conflict, Technol. Soc. 68 (2022) 101808.
[67] N. Shevchuk, V. Benson, H. Oinas-Kukkonen, Risk and self-disclosure in sustainable persuasive smart home technologies, in: AMCIS, 2019.
[68] N. Fruchter, I. Liccardi, Consumer attitudes towards privacy and security in home assistants, in: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, in: CHI EA '18, Association for Computing Machinery, New York, NY, USA, 2018, pp. 1–6, http://dx.doi.org/10.1145/3170427.3188448.
[69] G. Germanos, P. Light, R. Zoorob, J. Salemi, F. Khan, M. Hansen, K. Gupta, B. Trautner, L. Grigoryan, Validating use of electronic health data to identify patients with urinary tract infections in outpatient settings, Antibiotics (Basel) 9 (9) (2020) 536.
[70] N. Abdi, K.M. Ramokapane, J.M. Such, More than smart speakers: Security and privacy perceptions of smart home personal assistants, in: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security, SOUPS '19, USENIX Association, USA, 2019, pp. 451–466.
[71] J. Lau, B. Zimmerman, F. Schaub, Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers, Proc. ACM Hum.-Comput. Interact. 2 (CSCW) (2018) http://dx.doi.org/10.1145/3274371.
[72] X. Lei, G.-H. Tu, T. Xie, S. Wang, BFastPay: A routing-free protocol for fast payment in bitcoin network, in: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, CODASPY '21, Association for Computing Machinery, New York, NY, USA, 2021, pp. 77–87, http://dx.doi.org/10.1145/3422337.3447823.
[73] R. Mitev, M. Miettinen, A.-R. Sadeghi, Alexa Lied to me: Skill-based man-in-the-middle attacks on virtual assistants, in: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, in: Asia CCS '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 465–478, http://dx.doi.org/10.1145/3321705.3329842.
[74] A. Ponticello, M. Fassl, K. Krombholz, Exploring authentication for security-sensitive tasks on smart home voice assistants, in: Proceedings of the Seventeenth USENIX Conference on Usable Privacy and Security, SOUPS '21, USENIX Association, USA, 2023.
[75] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, B. Ur, Rethinking access control and authentication for the home internet of things (IoT), in: USENIX Security Symposium, 2018, pp. 255–272.
[76] J.S. Edu, J.M. Such, G. Suarez-Tangil, Smart home personal assistants: a security and privacy review, ACM Comput. Surv. 53 (6) (2020) 1–36.
[77] L. Hernández Acosta, D. Reinhardt, A survey on privacy issues and solutions for voice-controlled digital assistants, Pervasive Mob. Comput. 80 (2022) 101523, http://dx.doi.org/10.1016/j.pmcj.2021.101523, URL https://www.sciencedirect.com/science/article/pii/S1574119221001449.
[78] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, F. Qian, Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems, in: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 1381–1396.
[79] K. Painchaud, L. Deligiannidis, Customized services using voice assistants, in: 2020 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE, 2020, pp. 1060–1065.
[80] F. Brasser, T. Frassetto, K. Riedhammer, A.-R. Sadeghi, T. Schneider, C. Weinert, VoiceGuard: Secure and private speech processing, in: Interspeech, Vol. 18, 2018, pp. 1303–1307.
[81] A. Al-Husamiyah, M. Al-Bashayreh, A comprehensive acceptance model for smart home services, Int. J. Data Netw. Sci. 6 (1) (2022) 45–58.
[82] Y. Liu, Y. Gan, Y. Song, J. Liu, What influences the perceived trust of a voice-enabled smart home system: An empirical study, Sensors 21 (6) (2021) 2037.
[83] D. Wright, P. De Hert, Introduction to privacy impact assessment, in: D. Wright, P. De Hert (Eds.), Privacy Impact Assessment, Springer Netherlands, Dordrecht, 2012, pp. 3–32, http://dx.doi.org/10.1007/978-94-007-2543-0_1.
[84] M. Hubert, M. Blut, C. Brock, R.W. Zhang, V. Koch, R. Riedl, The influence of acceptance and adoption drivers on smart home usage, Eur. J. Mark. 53 (6) (2019) 1073–1098.
[85] R. Mulcahy, K. Letheren, R. McAndrew, C. Glavas, R. Russell-Bennett, Are households ready to engage with smart home technology? J. Mark. Manag. 35 (15–16) (2019) 1370–1400.
[86] W. Li, T. Yigitcanlar, I. Erol, A. Liu, Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework, Energy Res. Soc. Sci. 80 (2021) 102211.
[87] J. Markendahl, S. Lundberg, O. Kordas, S. Movin, On the role and potential of IoT in different industries: Analysis of actor cooperation and challenges for introduction of new technology, in: 2017 Internet of Things Business Models, Users, and Networks, IEEE, 2017.
[88] S. Cannizzaro, R. Procter, S. Ma, C. Maple, Trust in the smart home: Findings from a nationally representative survey in the UK, PLoS One 15 (5) (2020) e0231615.
[89] A.R. Rieks, J. Dedrick, J. Stanton, Risks, benefits, and control of information: Two studies of smart electric meter privacy, J. Assoc. Inf. Sci. Technol. 71 (9) (2020) 1060–1073.
[90] A. Shuhaiber, I. Mashal, Understanding users' acceptance of smart homes, Technol. Soc. 58 (101110) (2019) 101110.
[91] S. Cannizzaro, R. Procter, S. Ma, C. Maple, Adoption and acceptability of smart devices for the home, in: Living in the Internet of Things (IoT 2019), Institution of Engineering and Technology, 2019.
[92] L. Liu, M. Workman, S. Hayes, Net zero and the potential of consumer data - United Kingdom energy sector case study: The need for cross-sectoral best data practice principles, Energy Policy 163 (112803) (2022) 112803.
[93] G. Chalhoub, I. Flechais, N. Nthala, R. Abu-Salma, Innovation inaction or in action? The role of user experience in the security and privacy design of smart home cameras, in: Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security, SOUPS '20, USENIX Association, USA, 2020.
[94] J. Chen, L. Urquhart, 'They're all about pushing the products and shiny things rather than fundamental security':Mapping socio-technical challenges in securing the smart home, Inf. Commun. Technol. Law 31 (1) (2022) 99–122.
[95] B.K. Sovacool, D.D. Furszyfer Del Rio, Smart home technologies in europe: A critical review of concepts, benefits, risks and policies, Renew. Sustain. Energy Rev. 120 (109663) (2020) 109663.
[96] S. Piasecki, L. Urquhart, P.D. McAuley, Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards, Comput. Law Secur. Rep. 42 (105542) (2021) 105542.
[97] J. Chen, L. Edwards, L. Urquhart, D. McAuley, Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption, Int. Data Priv. Law 10 (4) (2021) 279–293.
[98] K. Mcmahon, Tell the smart house to mind its own business!: Maintaining privacy and security in the era of smart devices, 86 Fordham L, 86 Fordham L. Rev (2018).



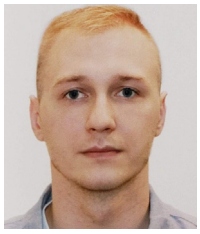
Dr. Shola Olabode (SO): Dr. SO is a research associate from Newcastle University interested in ICT political participation and civic engagement, online misinformation, disinformation and elections, digital activism, and cyberconflicts.



Rebecca Owens (RO): RO is a research assistant from Newcastle University who is interested in Intellectual property, competition law, as well as technology regulation and governance.

Viana Nijia Zhang (VNZ): VNZ is a research assistant from Newcastle University who is interested in human computer interaction research with a focus on digital health and digital education. She specifically works on mental health, emotional well-being, and chatbot related issues.

Dr. Jehana Copilah-Ali (JCA): Dr. JCA is a research associate from Newcastle University researching and advocating for Corporate Digital Responsibility (CDR) promoting ethical digital and data practices towards reducing complex online harms.



Dr. Maxim Kolomeets (MK): Dr. MK is a research associate from Durham University whose research interest is in cybersecurity with a focus on security of social media, risk analysis and data visualisation.

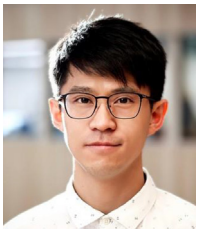
Dr. Han Wu (HW): Dr. HW is a research associate from Birmingham University whose research interest is in federated learning and cyber-security related topics.

Dr. Shrikant Malviya (SM): Dr. SM is a research associate from Durham University whose research interest is in natural language processing and voice assistant technology.

Karolina Markecviciute (KM): KM is a research assistant from Durham University whose research interest is in finance and cross-benefit analysis.

Dr. Tasos Spiliotopoulos (TS): Dr. TS is a Human-Computer Interaction researcher and an Innovation Fellow at the Centre for Digital Citizens. His research focuses on social technologies and human-centred design. Key topics in his research include privacy, trust, security, computational social science, computer-mediated communication, financial technologies, and digital identities.

Dr. Cristina Neesham (CN): Dr. CN is director of Business Ethics and Corporate Social Responsibility (CSR) at Newcastle University Business School, a reader in Business Ethics and CSR, and a Co-Investigator on the AGENCY project.



Dr. Lei Shi (LS): Lei Shi is a Senior Lecturer (Associate Professor) at Open Lab. His research interest lies in the improvement of interactions between humans and AI by integrating Human-Computer Interaction (HCI) approaches with Artificial Intelligence (AI) technologies that facilitate effective collaboration and co-creation. He is particularly interested in the empirical understanding of the future of AI-powered interactive systems with ethical, legal, and societal values, through developing and experimenting with intelligent software and hardware that enable and advance creativity, productivity, adaptability, participation, diversity, inclusion, and heterogeneity, in a range of areas including education, design, publicity, and wellbeing.

Professor Deborah Chambers (DC) is Professor of Media and Cultural Studies at Newcastle University and a Co-Investigator on the AGENCY project. Her research lies within two areas, intersecting media & cultural studies and sociology. The first is digital technologies and social relations: addressing the interconnections between media technologies, media cultures and everyday life. Her research focuses on the changing cultural forms and uses of media technologies, from early television to today's digital and smart technologies; the transforming role of media and digital technologies in homes and households; social media, mobility and networked intimacies; families, children and media.