Smart Home Privacy: A Scoping Review

Ali Ahmed[1][a], Victor Ungureanu[2][b], Tarek Gaber[3][c], Craig Watterson[1][d] and Fatma Masmoudi[4][e]

[1]*Victoria University of Wellington, Kelburn Parade, Wellington, 6012, New Zealand*

[2]*University of Liverpool, Sutton, England, U.K.*

[3]*University of Salford, 43 Crescent, Salford, M5 4WT, Greater Manchester, U.K.*

[4]*Prince Sattam Bin Abdulaziz University, Alkharj, 11942, Saudi Arabia*

Keywords: Smart Homes, Privacy, Scoping Survey, Data Collection, User Consent, Data Anonymisation.

Abstract: Privacy concerns in smart home technologies have surged as their adoption becomes ubiquitous. This scoping review paper undertakes an exhaustive examination of the current literature to elucidate the state of privacy within this burgeoning context. Employing a scoping review methodology, we have analysed about 78 peer-reviewed articles. Key emergent themes include privacy concerns, trust, user perception, and a range of technical risks and mitigation. Our findings reveal significant gaps in privacy design and protection, establishing this paper as a novel contribution that sets the groundwork for future research. Additionally, it provides practitioners and policymakers with actionable insights for enhancing privacy measures in smart homes. Supplemental material, including a curated database of the reviewed literature and previously published papers, will be available to reviewers to enrich the understanding of our contribution.

1 INTRODUCTION

Smart home technologies have experienced unprecedented growth and integration into our daily lives, revolutionising how we interact with our living spaces (Deschamps-Sonsino, 2018, page 8). These interconnected devices offer convenience, energy efficiency, and enhanced security. However, this rapid proliferation of smart home systems has raised significant privacy concerns, as these devices collect and process vast amounts of personal data (Ziegeldorf et al., 2014). This paper aims to provide a scoping survey of the existing literature on privacy in smart homes, shedding light on the various dimensions of this critical issue. This paper aims to contribute to understanding smart home privacy challenges and identify avenues for further research.

One of the primary privacy concerns in smart homes revolves around collecting and using personal data. Smart home devices like voice assistants, smart meters, and sensors can capture sensitive information, including audio recordings, video feeds, energy consumption patterns, and user behaviour (Sharif and Tenbergen, 2020). The potential for unauthorised access, data breaches, or misuse of this data raises significant ethical and legal concerns. Furthermore, sharing personal data by smart home devices with third parties introduces additional privacy risks (Edu et al., 2020). Service providers, manufacturers, and advertisers may have access to sensitive information, leading to potential profiling, targeted advertising, or even surveillance. The lack of transparency regarding data-sharing practices and the potential for data aggregation across multiple devices further exacerbate these concerns. User consent and control over personal data in smart homes are critical aspects of privacy protection. However, it is often challenging for users to understand the full extent of data collection and make informed decisions regarding consent. Smart home platforms ' privacy policies and consent mechanisms may be complex and difficult to comprehend, leading to potential gaps in user understanding and control over personal information.

Various technical and policy solutions have been proposed to address these privacy challenges. Data anonymisation techniques, encryption protocols, and

[a] https://orcid.org/0000-0002-7370-3044
[b] https://orcid.org/0009-0000-6561-6939
[c] https://orcid.org/0000-0003-4065-4191
[d] https://orcid.org/0000-0001-9471-6015
[e] https://orcid.org/0000-0002-7339-3349

Ahmed, A., Ungureanu, V., Gaber, T., Watterson, C. and Masmoudi, F.
Smart Home Privacy: A Scoping Review.
DOI: 10.5220/0012255900003648
In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 635-642
ISBN: 978-989-758-683-5; ISSN: 2184-4356

access control mechanisms aim to protect personal information while allowing the benefits of smart home technologies to be realised. Additionally, regulatory frameworks and industry standards have been developed to ensure privacy protection in smart home ecosystems. By conducting a scoping review, this paper aims to identify the current state of knowledge, highlight research trends, and identify gaps that require further investigation. The findings of this paper contributes to the ongoing discussions on smart home privacy, informing policymakers, industry practitioners, and researchers about the key issues at hand and fostering the development of privacy-preserving solutions.

The organisation of this paper is as follows:

1. Section 2 introduces the research methodology.
2. Section 3 introduces the individual studies that have been surveyed and provided a summary of those studies.
3. Section 4 identifies the common themes in literature and answers the research question.
4. Section 5 highlights the limitations of this study.
5. Section 6 concludes the paper and highlights possible future research.

2 RESEARCH METHODOLOGY

The objective of this scoping review is to map the existing literature on the topic of smart home privacy. The review aims to identify and analyse the key concepts, sources of evidence, and research gaps related to privacy concerns in smart-home technologies. The question, "What are the main dimensions of privacy concerns in the context of smart homes?" guided this scoping review. The question seeks to identify and understand the primary aspects or dimensions related to privacy concerns. In the context of smart homes, these dimensions could include factors such as data collection, surveillance, information sharing, security vulnerabilities, user awareness, and control over personal information. The research question served as a guiding principle throughout the scoping review process. It helped focus the search strategy, select appropriate inclusion and exclusion criteria, and systematically assess and synthesise the findings from the identified studies. By using this question as a starting point, this paper aimed to ensure that the scoping review covered a broad range of privacy dimensions and addressed the diversity of concerns within the context of smart homes.

To ensure a comprehensive search for relevant literature, the following databases is searched: IEEE Xplore, ACM Digital Library, Springer, and Google Scholar. The search terms and keywords to be used include variations and combinations of: "smart home", "privacy", "data protection", "security", "personal information", "internet of things", "smart devices" and "ethics".

The inclusion and exclusion criteria for the selection of articles are as follows:

Table 1: Inclusion and Exclusion Criteria.

Criteria	Description
Inclusion	Articles that focus on privacy concerns in the context of smart-home technologies. Articles that present empirical research, theoretical frameworks, conceptual models, or practical approaches to smart home privacy. Articles published in the English language. Articles published from 2010 to 2023.
Exclusion	Articles that do not specifically address smart homes privacy. Articles that are not peer-reviewed. Articles published in languages other than English.

The study selection process involves title/abstract screening and full-text screening. During the title/abstract screening, articles that do not meet the inclusion criteria will be excluded. In the full-text screening, the reviewers will assess the remaining articles against the inclusion and exclusion criteria to select the final articles for data extraction and analysis.

Zotero[1] is used to extract relevant information from the selected articles. The data to be extracted may include the author(s), year of publication, research methods, sample size, key findings, any frameworks or models discussed, and possible auto-generated tags. Afterwards, thematic analysis will be employed to identify the main themes, concepts, and dimensions related to smart home privacy.

Given the scoping nature of this review, a formal quality assessment of individual studies will not be conducted. Instead, the included articles will be assessed for relevance to the research question and its contribution to understanding smart home privacy.

[1] https://www.zotero.org, last accessed 18 June 2023

3 LITERATURE SURVEY: INDIVIDUAL STUDIES

In the study by (Lin and Bergmann, 2016), the authors emphasised the prevalence of privacy risks in smart homes, underscoring the challenges arising from the lack of expertise and standardisation. Their advocacy for auto-configuration and automatic updates in smart appliances aimed to mitigate these risks. (Liu et al., 2022) highlighted the necessity for Smart Home Privacy Protection (SHPP) standards as crucial for societal development. This emphasises the need for a structured framework to address privacy concerns in smart home ecosystems. Proposing innovative solutions, (Alhazmi et al., 2022) introduced the MQTT-Based Privacy Orchestrator (MPO). This solution aims to comprehensively address security and privacy concerns, targeting key barriers to consumer adoption of IoT devices. (Vö et al., 2017) delved into optimising Wake-Up-Word (WUW) detection in voice-activated smart homes, proposing an architecture that prioritises low-cost integration, privacy, and ease of use. This signifies a significant step towards ensuring secure voice interactions within smart home environments. The comprehensive analysis conducted by (Ford and Palmer, 2019) on the Alexa app and devices revealed privacy issues related to command logging accuracy and potential unauthorised recordings. The study's suggestion to process voice commands within the smart home network presents a viable solution to enhance user privacy. Studies such as (Abdallah et al., 2020) and (Guhr et al., 2020) explore the intersection of smart home technology with specialised applications, catering to the elderly and assessing the impact of privacy concerns on device adoption, respectively. Additionally, (Zhang et al., 2020) introduces a blockchain-based solution to optimise energy consumption and enhance privacy in power data exchange. In addressing privacy challenges, (Apthorpe et al., 2018) revisited traffic padding methods, proposing Stochastic Traffic Padding (STP) as an effective solution. Simultaneously, (Hatamian, 2020) provided a privacy and security principles catalogue for app developers, offering practical guidance. Furthermore, (Musto et al., 2021) outlined a strategy for personalised service access, while (Rios et al., 2021) introduced a Privacy Manager based on Edge Computing (PMEC) to enhance data privacy in IoT settings. Finally, (Qashlan et al., 2021) explored data security through blockchain, integrating attribute-based access control and edge computing.

The study by (Vimalkumar et al., 2021) investigated factors influencing user trust in Voice-based Digital Assistants, shedding light on the significance of perceived risk and trust in shaping user perceptions and adoption. (Haney and Furman, 2022) explored the importance of smart home updates and the link between these updates and privacy/security. This highlights the need for transparent communication between users and developers regarding the impact of updates on privacy. Investigations by (Li et al., 2023) into the privacy concerns of new purchasers of smart home devices and (Zou et al., 2023)'s demonstration of IoTBeholder's effectiveness in predicting user behaviour showcase the evolving landscape of privacy considerations and predictive technologies in smart homes.

(Pierce et al., 2022) addressed privacy concerns in IoT devices, focusing on potential compromises to individual privacy posed by spatial sensors. This emphasises the importance of ensuring user privacy in the evolving landscape of IoT. (Nassiri Abrishamchi et al., 2022) delved into side-channel attacks, specifically Fingerprint and Timing-based Snooping (FATS), proposing solutions to secure smart homes against these passive assaults. This research contributes to the ongoing efforts to fortify IoT devices against emerging privacy threats. (Mohanty et al., 2022) conducted a large-scale study on privacy concerns in IoT devices, exploring factors like anonymity and GDPR compliance. The study's self-assessment scorecard offers a practical tool for mitigating privacy risks in IoT settings.

(Musale and Lee, 2023) examined the impact of cloud-based Trusted Execution Environments (TEEs) in IoT devices, revealing insights into user comfort in data collection. This highlights the nuanced relationship between technology and user perception in the context of privacy. The exploration by (Windl et al., 2023) into the need for tangible privacy mechanisms in smart homes underscores the importance of incorporating tangible elements, such as tokens for privacy preferences and dashboards for device overviews, to enhance user awareness and control in complex environments.

4 DISCUSSION

Figure 1 depicts the word frequency distribution within the analysed literature. It is the first step in providing insights into the prevalent themes and concepts related to smart homes and privacy concerns. From Figure 1, one can discern that the text emphasises topics such as privacy, concerns, and user expectations in the context of smart homes. Additionally, it highlights the significance of privacy-preserving technologies and the need for measures and countermea-

Figure 1: Literature Word Analysis.

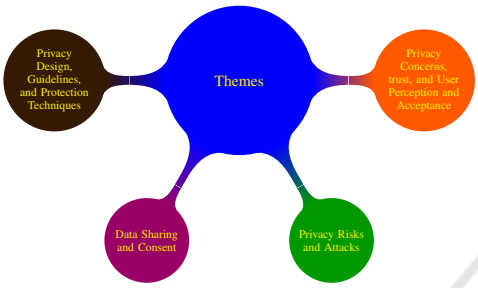

Figure 2: Smart-home Privacy: Themes.

sures to address perceived risks.

Given that and guided by the research question, the literature survey shows common Themes and categories in smart home privacy research. These categories capture the common themes that emerge from the studies survey in this paper as seen in Table 2 and Figure 2.

Privacy Concerns, Trust and User Perception and Acceptance. Research on privacy concerns in smart home environments broadly focuses on three areas: risk perception, privacy threats, and user attitudes. Studies such as (Guhr et al., 2020), (Balasubramanian et al., 2021), and (Kreuter et al., 2020) investigated the factors that influence users' perceptions of privacy risks. Another avenue of inquiry, represented by (Haney and Furman, 2022), (Vimalkumar et al., 2021), and (Mohanty et al., 2022), examines the impact of privacy threats on user behaviour and technology adoption. The relationship between privacy concerns and user intentions has also been explored, as evidenced by (Windl et al., 2023).

In summary, this body of work enhances our understanding of users' privacy concerns, risk perceptions, and attitudes towards smart home technologies. The insights gained can guide the development of user-centric design approaches, privacy-enhancing strategies, and effective communication methods to improve the acceptance of smart home devices. Furthermore, the researchers on user attitudes towards privacy in smart homes has illuminated key factors af-

Table 2: Themes and Corresponding Papers.

Theme	Individual Papers
Privacy Concerns, Trust, and User Perception and Acceptance	(Guhr et al., 2020; Balasubramanian et al., 2021; Kreuter et al., 2020; Haney and Furman, 2022; Vimalkumar et al., 2021; Windl et al., 2023; Zheng et al., 2018; Haney et al., 2021; Schomakers et al., 2021; Yao et al., 2019b; Abdi et al., 2019; Haney et al., 2020; Tabassum et al., 2019; Georgiev and Schlögl, 2018; Wilkowska et al., 2015; Schomakers et al., 2020; Almutairi and Almarhabi, 2021; Kaaz et al., 2017; Liu et al., 2021; Shouran et al., 2019; Shuhaiber et al., 2023)
Privacy Risk and Attacks	(Setayeshfar et al., 2021; Zou et al., 2023; Musto et al., 2021; Pierce et al., 2022; Nassiri Abrishamchi et al., 2022; Edu et al., 2020; Al-Turjman et al., 2022; Habibzadeh et al., 2019; Tabassum et al., 2019; Nemec Zlatolas et al., 2022; Duezguen et al., 2021; Leitão, 2019; Acar et al., 2020; Hafeez et al., 2019; Ramapatruni et al., 2019; Yakubu et al., 2023; Ozmen et al., 2023)
Data Sharing and Consent	(Mohanty et al., 2022; Seymour et al., 2023; Siddiqui et al., 2023; Zampati, 2023; Khan et al., 2020; Sultana et al., 2020; Singh et al., 2019; Lin et al., 2019; Zhang et al., 2023)
Privacy Design, Guidelines, and Protection Techniques	(Zhang et al., 2020; Zou et al., 2023; Hatamian, 2020; Musto et al., 2021; Rios et al., 2021; Qashlan et al., 2021; Makhdoom et al., 2020; Sultana et al., 2020; Singh et al., 2019; Lin et al., 2019; Iqbal et al., 2023; Poh et al., 2019; She et al., 2019; Yao et al., 2019a; Aïvodji et al., 2019; Wan et al., 2020; Hafeez et al., 2019; Ramapatruni et al., 2019; Augusto-Gonzalez et al., 2019; Khanpara et al., 2023; Yakubu et al., 2023; Ozmen et al., 2023)

fecting privacy-related decisions. These insights are instrumental for developing privacy-enhancing measures and user-centric designs, ultimately fostering greater acceptance of smart home technologies.

Privacy Risks and Attacks. Several studies have explored the security and privacy implications in smart homes. For instance, (Setayeshfar et al., 2021) revealed vulnerabilities through machine learning analyses of IoT signals. (Zou et al., 2023) considered blockchain for enhanced privacy, while (Musto et al., 2021) focused on distributed identity management. Additional risks like DDoS and firmware issues were also documented (Saxena et al., 2020; Guhr et al., 2020; Buil-Gil et al., 2023).

Data Sharing and Consent. Some studies have investigated the factors affecting users' willingness to share data in smart homes, including the role of privacy regulations. (Seymour et al., 2023) specifically examined how GDPR influences trust and data-sharing behaviour. User preferences and personality traits are key in shaping data-sharing behaviour in smart homes. (Siddiqui et al., 2023) explored the role of control, perceived benefits, and transparency in data-sharing decisions. (Zampati, 2023) looked into how personality traits like privacy concerns and risk perception influence willingness to share data. These insights could guide the development of tailored privacy mechanisms and policies for smart homes.

Privacy Design, Guidelines and Protection Techniques. Several studies have proposed techniques to enhance user privacy in smart homes. (Zhang et al., 2020) and (Zou et al., 2023) focused on blockchain technology to ensure data integrity and confidentiality. (Hatamian, 2020) and (Musto et al., 2021) looked into distributed authentication mechanisms for secure user control. Context-aware policy languages were explored by (Rios et al., 2021) and (Qashlan et al., 2021) for fine-grained data access control. Cloud-based trusted environments were investigated by (Makhdoom et al., 2020) and (Sultana et al., 2020) to secure user data. These contributions aim to develop robust privacy-enhancing solutions for smart homes.

5 LIMITATIONS OF THE STUDY

The search strategy is limited by the specific choice of keywords and may miss some relevant studies. The article selection criteria, focusing on aspects like privacy in smart homes and English language, could also exclude pertinent work, thus affecting the review's comprehensiveness. Additionally, the absence of a formal quality assessment of included studies may question the overall reliability of the findings. Therefore, the results may lack generalisability across the broader ecosystem of smart home privacy issues.

While the inclusion of variations and combinations of search terms is a good starting point, there is a possibility that some relevant studies may not be captured due to the specific choice of keywords. The effectiveness of the search strategy in retrieving comprehensive results may depend on the relevance and appropriateness of the chosen terms. The criteria for article selection are focused on specific aspects, such as privacy concerns in smart-home technologies, empirical research, theoretical frameworks, and articles published in English. While these criteria help narrow down the scope, they may also exclude relevant studies that fall outside these specific criteria, potentially limiting the comprehensiveness of the scoping review. The methodology states that a formal quality assessment of individual studies will not be conducted. While this is acceptable for a scoping review, it means that the included articles' quality and potential biases are not thoroughly evaluated, which may impact the overall reliability of the findings. Given the aforementioned limitations, this study's findings may lack generalisability to other areas of smart homes and may not capture the broader landscape of privacy issues that exist within the entire ecosystem of smart home devices and systems.

6 CONCLUSION AND FUTURE WORK

In summary, this scoping review offers a thorough assessment of existing studies on privacy issues in smart homes, identifying key themes like trust, user perception, risks, and protective measures. The findings stress the urgency for continued research to address these privacy concerns as smart home adoption expands. Standardised privacy guidelines and user-centric design are emphasised for ensuring trust, data security, and ethical practices. Future research should delve into user perceptions and trust to inform the development of privacy-focused features. As smart home technology evolves, ongoing studies should explore emerging privacy risks and the influence of new technologies like AI and IoT on smart home privacy.

REFERENCES

Abdallah, N. H., Affes, E., Bouslimani, Y., Ghribi, M., Kaddouri, A., and Ghariani, M. (2020). Smart assistant robot for smart home management. In *2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)*, pages 317–321. IEEE.

Abdi, N., Ramokapane, K. M., and Such, J. M. (2019). 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, page 451–466, USA. USENIX Association.

Acar, A., Fereidooni, H., Abera, T., Sikder, A. K., Miettinen, M., Aksu, H., Conti, M., Sadeghi, A.-R., and Uluagac, S. (2020). Peek-a-boo: I see your smart home activities, even encrypted! In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 207–218.

Aïvodji, U. M., Gambs, S., and Martin, A. (2019). Iotfla: A secured and privacy-preserving smart home architecture implementing federated learning. In *2019 IEEE security and privacy workshops (SPW)*, pages 175–180. IEEE.

Al-Turjman, F., Zahmatkesh, H., and Shahroze, R. (2022). An overview of security and privacy in smart cities' iot communications. *Transactions on Emerging Telecommunications Technologies*, 33(3):1–19.

Alhazmi, A., Alawaji, K., and OConnor, T. (2022). Mpo: Mqtt-based privacy orchestrator for smart home users. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 988–993. IEEE.

Almutairi, O. and Almarhabi, K. (2021). Investigation of smart home security and privacy: Consumer perception in saudi arabia. *International Journal of Advanced Computer Science and Applications*, 12(4).

Apthorpe, N., Huang, D. Y., Reisman, D., Narayanan, A., and Feamster, N. (2018). Keeping the smart home private with smart (er) iot traffic shaping. *arXiv preprint arXiv:1812.00955*, page 128–148.

Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Anagnostopoulos, M., Spathoulas, G., Giannoutakis, K. M., Votis, K., Tzovaras, D., Genge, B., Gelenbe, E., et al. (2019). From internet of threats to internet of things: A cyber security architecture for smart homes. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–6. IEEE.

Balasubramanian, G. V., Beaney, P., and Chambers, R. (2021). Digital personal assistants are smart ways for assistive technology to aid the health and wellbeing of patients and carers. *BMC geriatrics*, 21:1–10.

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., and Nicholson, J. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior*, 145:107770.

Deschamps-Sonsino, A. (2018). *Smarter homes: how technology has changed your home life*. Apress.

Duezguen, R., Mayer, P., Berens, B., Beckmann, C., Aldag, L., Mossano, M., Volkamer, M., and Strufe, T. (2021). How to increase smart home security and privacy risk perception. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 997–1004. IEEE.

Edu, J. S., Such, J. M., and Suarez-Tangil, G. (2020). Smart home personal assistants: a security and privacy review. *ACM Computing Surveys (CSUR)*, 53(6):1–36.

Ford, M. and Palmer, W. (2019). Alexa, are you listening to me? an analysis of alexa voice service network traffic. *Personal and ubiquitous computing*, 23:67–79.

Georgiev, A. and Schlögl, S. (2018). Smart home technology: An exploration of end user perceptions. *Innovative Lösungen für eine alternde Gesellschaft: Konferenzbeiträge der SMARTER LIVES*, 18(20.02):2018.

Guhr, N., Werth, O., Blacha, P. P. H., and Breitner, M. H. (2020). Privacy concerns in the smart home context. *SN Applied Sciences*, 2:1–12.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., and Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, 50:101660.

Hafeez, I., Antikainen, M., and Tarkoma, S. (2019). Protecting iot-environments against traffic analysis attacks with traffic morphing. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 196–201. IEEE.

Haney, J. and Furman, S. (2022). User perceptions and experiences with smart home updates. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 782–799. IEEE Computer Society.

Haney, J. M., Acar, Y., and Furman, S. (2021). " it's the company, the government, you and i": User perceptions of responsibility for smart home privacy and security. In *USENIX Security Symposium*, pages 411–428.

Haney, J. M., Furman, S. M., and Acar, Y. (2020). Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, pages 393–411. Springer.

Hatamian, M. (2020). Engineering privacy in smartphone apps: A technical guideline catalog for app developers. *IEEE Access*, 8:35429–35445.

Iqbal, W., Abbas, H., Deng, P., Wan, J., Rauf, B., Abbas, Y., and Rashid, I. (2023). Alam: Anonymous lightweight authentication mechanism for sdn enabled smart homes. *Journal of Network and Computer Applications*, page 103672.

Kaaz, K. J., Hoffer, A., Saeidi, M., Sarma, A., and Bobba, R. B. (2017). Understanding user perceptions of privacy, and configuration challenges in home automation. In *2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pages 297–301. IEEE.

Khan, M. A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M. I., Nasser, N., and Ali, A. (2020). A machine learning approach for blockchain-based smart home networks security. *IEEE Network*, 35(3):223–229.

Khanpara, P., Lavingia, K., Trivedi, R., Tanwar, S., Verma, A., and Sharma, R. (2023). A context-aware internet of things-driven security scheme for smart homes. *Security and Privacy*, 6(1):e269.

Kreuter, F., Haas, G.-C., Keusch, F., Bähr, S., and Trappmann, M. (2020). Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. *Social Science Computer Review*, 38(5):533–549.

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*, pages 527–539.

Li, L., Li, T., Cai, H., Zhang, J., and Wang, J. (2023). I will only know after using it: The repeat purchasers of smart home appliances and the privacy paradox problem. *Computers & Security*, 128:103156.

Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., and Choo, K.-K. R. (2019). Homechain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, 7(2):818–829.

Lin, H. and Bergmann, N. W. (2016). Iot privacy and security challenges for smart home environments. *Information*, 7(3):44.

Liu, D., Wu, C., Yang, L., Zhao, X., and Sun, Q. (2022). The development of privacy protection standards for smart home. *Wireless Communications and Mobile Computing*, 2022.

Liu, Y., Gan, Y., Song, Y., and Liu, J. (2021). What influences the perceived trust of a voice-enabled smart home system: An empirical study. *Sensors*, 21(6):2037.

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., and Ni, W. (2020). Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, 88:101653.

Mohanty, S., Cormican, K., and Dhanapathi, C. (2022). Analysis of critical success factors to mitigate privacy risks in iot devices. *Procedia Computer Science*, 196:191–198.

Musale, P. and Lee, A. J. (2023). Trust tee?: Exploring the impact of trusted execution environments on smart home privacy norms. *Proceedings on Privacy Enhancing Technologies*, 3:5–23.

Musto, C., Narducci, F., Polignano, M., De Gemmis, M., Lops, P., and Semeraro, G. (2021). Myrrorbot: A digital assistant based on holistic user models for personalized access to online services. *ACM Transactions on Information Systems (TOIS)*, 39(4):1–34.

Nassiri Abrishamchi, M. A., Zainal, A., Ghaleb, F. A., Qasem, S. N., and Albarrak, A. M. (2022). Smart home privacy protection methods against a passive wireless snooping side-channel attack. *Sensors*, 22(21):8564.

Nemec Zlatolas, L., Feher, N., and Hölbl, M. (2022). Security perception of iot devices in smart homes. *Journal of Cybersecurity and Privacy*, 2(1):65–73.

Ozmen, M. O., Song, R., Farrukh, H., and Celik, Z. B. (2023). Evasion attacks and defenses on smart home physical event verification. In *30th Annual Network and Distributed System Security Symposium, NDSS 2023, San Diego, California, USA, February 27 - March 3, 2023*, pages 1–18. The Internet Society.

Pierce, J., Weizenegger, C., Nandi, P., Agarwal, I., Gram, G., Hurrle, J., Liao, H., Lo, B., Park, A., Phan, A., et al. (2022). Addressing adjacent actor privacy: Designing for bystanders, co-users, and surveilled subjects of smart home cameras. In *Designing Interactive Systems Conference*, pages 26–40.

Poh, G. S., Gope, P., and Ning, J. (2019). Privhome: Privacy-preserving authenticated communication in smart home environment. *IEEE Transactions on Dependable and Secure Computing*, 18(3):1095–1107.

Qashlan, A., Nanda, P., He, X., and Mohanty, M. (2021). Privacy-preserving mechanism in smart home using blockchain. *IEEE Access*, 9:103651–103669.

Ramapatruni, S., Narayanan, S. N., Mittal, S., Joshi, A., and Joshi, K. (2019). Anomaly detection models for smart home security. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 19–24. IEEE.

Rios, R., Onieva, J. A., Roman, R., and Lopez, J. (2021). Personal iot privacy control at the edge. *IEEE Security & Privacy*, 20(1):23–32.

Saxena, U., Sodhi, J., and Singh, Y. (2020). An analysis of ddos attacks in a smart home networks. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pages 272–276.

Schomakers, E.-M., Biermann, H., and Ziefle, M. (2020). Understanding privacy and trust in smart home environments. In *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, pages 513–532. Springer.

Schomakers, E.-M., Biermann, H., and Ziefle, M. (2021). Users' preferences for smart home automation–investigating aspects of privacy and trust. *Telematics and Informatics*, 64:101689.

Setayeshfar, O., Subramani, K., Yuan, X., Dey, R., Hong, D., Lee, K. H., and Kim, I. K. (2021). Chatterhub: Privacy invasion via smart home hub. In *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 181–188.

Seymour, W., Cote, M., and Such, J. (2023). Legal obligation and ethical best practice: Towards meaningful verbal consent for voice assistants. In *Proceedings of the Conference on Human Factors in Computing Systems CHI '23*, pages 1–16, New York, NY, USA. Association for Computing Machinery.

Sharif, K. and Tenbergen, B. (2020). Smart home voice assistants: a literature survey of user privacy and security vulnerabilities. *Complex Systems Informatics and Modeling Quarterly*, 24:15–30.

She, W., Gu, Z.-H., Lyu, X.-K., Liu, Q., Tian, Z., and Liu, W. (2019). Homomorphic consortium blockchain for smart home system sensitive data privacy preserving. *IEEE Access*, 7:62058–62070.

Shouran, Z., Ashari, A., and Priyambodo, T. (2019). Internet of things (iot) of smart home: privacy and security. *International Journal of Computer Applications*, 182(39):3–8.

Shuhaiber, A., Alkarbi, W., and Almansoori, S. (2023). Trust in smart homes: The power of social influences and perceived risks. In *Intelligent Sustainable Systems: Selected Papers of WorldS4 2022, Volume 1*, pages 305–315. Springer.

Siddiqui, S., Hameed, S., Shah, S. A., Khan, A. K., and Aneiba, A. (2023). Smart contract-based security architecture for collaborative services in municipal smart cities. *Journal of Systems Architecture*, 135:102802.

Singh, S., Ra, I.-H., Meng, W., Kaur, M., and Cho, G. H. (2019). Sh-blockcc: A secure and efficient internet of things smart home architecture based on cloud computing and blockchain technology. *International Journal of Distributed Sensor Networks*, 15(4):1–18.

Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., and Javaid, N. (2020). Data sharing system integrating access control mechanism using blockchain-based smart contracts for iot devices. *Applied Sciences*, 10(2):488–508.

Tabassum, M., Kosiński, T., and Lipford, H. R. (2019). "i don't own the data": End user perceptions of smart home device data practices and risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, page 435–450, USA. USENIX Association.

Vimalkumar, M., Sharma, S. K., Singh, J. B., and Dwivedi, Y. K. (2021). 'okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, 120:106763.

Vö, B., Schubert, T., and Becker, B. (2017). ihouse: A voice-controlled, centralized, retrospective smart home. In Magno, M., Ferrero, F., and Bilas, V., editors, *Sensor Systems and Software*, pages 68–80, Cham. Springer International Publishing.

Wan, Y., Xu, K., Xue, G., and Wang, F. (2020). Iotargos: A multi-layer security monitoring system for internet-of-things in smart homes. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pages 874–883. IEEE.

Wilkowska, W., Ziefle, M., and Himmel, S. (2015). Perceptions of personal privacy in smart home technologies: do user assessments vary depending on the research method? In *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3*, pages 592–603. Springer.

Windl, M., Schmidt, A., and Feger, S. S. (2023). Investigating tangible privacy-preserving mechanisms for future smart homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–16.

Yakubu, B. M., Khan, M. I., Khan, A., Jabeen, F., and Jeon, G. (2023). Blockchain-based ddos attack mitigation protocol for device-to-device interaction in smart home. *Digital Communications and Networks*.

Yao, Y., Basdeo, J. R., Kaushik, S., and Wang, Y. (2019a). Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*, pages 1–12.

Yao, Y., Basdeo, J. R., Mcdonough, O. R., and Wang, Y. (2019b). Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24.

Zampati, F. (2023). Ethical and legal considerations in smart farming: A farmer's perspective. *Towards Responsible Plant Data Linkage: Data Challenges for Agricultural Research and Development*, pages 257–272.

Zhang, F., Pan, Z., and Lu, Y. (2023). Aiot-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. *Information & Management*, 60(2):103736.

Zhang, S., Rong, J., and Wang, B. (2020). A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain. *International Journal of Electrical Power & Energy Systems*, 121:106140.

Zheng, S., Apthorpe, N., Chetty, M., and Feamster, N. (2018). User perceptions of smart home iot privacy. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–20.

Ziegeldorf, J. H., Morchon, O. G., and Wehrle, K. (2014). Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 7(12):2728–2742.

Zou, Q., Li, Q., Li, R., Huang, Y., Tyson, G., Xiao, J., and Jiang, Y. (2023). Iotbeholder: A privacy snooping attack on user habitual behaviors from smart home wi-fi traffic. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 7(1):1–26.