Privacy Concerns in the Age of Smart Home Devices

Nikita Vishvakarma[1], Nisha Yadav[2], Diya Verma[3]
[1,2,3] CSE(AI), Rajasthan College of Engineering for Women, Jaipur, India

Abstract: The connection of home electronic devices to the internet allows remote control of physical devices and involves the collection of large volumes of data. With the increase in the uptake of Internet-of-Things home devices, it becomes critical to understand the digital harms of smart homes. We present a systematic literature review on the security and privacy harms of smart homes. PRISMA methodology is used to systematically review 63 studies published between January 2011 and October 2021; and a review of known cases is undertaken to illustrate the literature review findings with real-world scenarios. Published literature identifies that smart homes may pose threats to confidentiality (unwanted release of information), authentication (sensing information being falsified) and unauthorised access to system controls. Most existing studies focus on privacy intrusions as a prevalent form of harm against smart homes. Other types of harms that are less common in the literature include hacking, malware and DoS attacks. Digital harms, and data associated with these harms, may vary extensively across smart devices. Most studies propose technical measures to mitigate digital harms, while fewer consider social prevention mechanisms. We also identify salient gaps in research, and argue that these should be addressed in future cross disciplinary research initiatives.

Keywords: ***Smart Homes, Internet of Things (IoT), Digital Harms, Security and Privacy Cybersecurity***

I. INTRODUCTION

This article presents a systematic review of the privacy and security harms associated with smart homes—physical devices connected via the Internet-of-Things (IoT). Originating in the early 1980s with Carnegie Mellon University's internet-connected Coca-Cola vending machine, IoT has expanded to include corporate systems, cars, grids, military tools, and home appliances. The term "smart home" (Lutolf, 1992) refers to internet-connected domestic devices like smart TVs, thermostats, speakers, locks, and voice assistants (e.g., Google Home, Amazon Alexa). These devices automate tasks and monitor household activity, forming interconnected ecosystems. A 2021 UK survey by tech UK and GfK showed high adoption rates: 58% owned smart TVs, 39% smart speakers, and 15% smart thermostats; by March 2022, 51% of UK meter readers were smart or advanced meters (BEIS, 2022).

However, smart homes pose risks to confidentiality, authentication, and access (Lin & Bergmann, 2016). Breaches may expose electricity usage patterns (Blythe & Johnson, 2021), sensitive medical data (Tzezana, 2016), or enable unauthorized control of appliances (Jacobsson et al., 2016). They may also facilitate cyberstalking and household power imbalances (Nicholls et al., 2020). Building on reviews by Marikyan et al. (2019) and Blythe & Johnson (2021), this article classifies digital harms, identifies vulnerable devices, and explores mitigation strategies. It supports Nord et al.'s (2019) model linking stakeholder priorities, device networks, and trust, contributing to IoT adoption theory.

II. LITERATURE REVIEW

1. Growing User Anxiety:

- A 2025 Copeland survey of 2,000 U.S. homeowners revealed a sharp rise in privacy concerns despite increased adoption of smart home tech like thermostats, TVs, and appliances.
- Users are more aware of how their data is collected, stored, and potentially shared—especially with the rise of AI-driven features.

2. Data Collection & Surveillance Risks:

- Smart devices continuously collect data such as voice commands, location, behavioral patterns, and even biometric information.
- Many users are unaware of the full extent of data being gathered or how it's used by manufacturers or third parties.

3. AI and Predictive Profiling:

- AI-enabled devices can infer sensitive personal details from usage patterns—like daily routines, emotional states, or health indicators.
- This raises ethical concerns about profiling and manipulation, especially when data is used for targeted advertising or sold to third parties.

4. Security Vulnerabilities:

- A 2023 international study found that many IoT devices in smart homes lack robust security protocols, making them vulnerable to hacking and unauthorized access.
- Weak passwords, outdated firmware, and lack of encryption are common issues.

5. Transparency & Consent Challenges:

- Privacy policies are often vague or overly technical, making it hard for users to give informed consent.
- Users may unknowingly agree to data sharing with advertisers, analytics firms, or cloud services.

6. Mitigation Strategies:

- Experts recommend:
  - Using devices from reputable brands with clear privacy commitments.
  - Regularly updating firmware and changing default passwords.
  - Reviewing privacy settings and disabling unnecessary data collection.
  - Using local storage options when available instead of cloud-based services.

Smart Home Privacy in Student & Professional Spaces:
For Students

- Shared Living Risks: In hostels or PGs, smart speakers or cameras may be installed by landlords or roommates. Students often don't control these devices, raising consent and surveillance issues.
- Academic Integrity: Devices with microphones (like Alexa or Google Home) could inadvertently record sensitive discussions—project ideas, exam prep, or personal struggles.
- Digital Footprint Awareness: Students may not realize how much data is collected—voice commands, sleep patterns, even emotional tone—and how it could be used by third parties.

For Professionals

- Work-from-Home Vulnerabilities: Smart assistants in home offices may overhear confidential meetings or client calls, risking data leaks.
- Hybrid Workspaces: Professionals using smart lighting, thermostats, or security systems in co-working spaces may face privacy breaches if devices are not properly secured.
- Behavioural Profiling: Usage data from smart devices can be used to infer productivity patterns, stress levels, or even leadership traits—raising ethical concerns in performance evaluations.

III. PROPOSED WORK

What You Can Do:

- Educate through sessions: Host awareness workshops on digital privacy and ethical tech use.
- Promote secure practices: Encourage students and professionals to:
  - Disable unnecessary features (like voice recording history).
  - Use guest modes or device-free zones during sensitive work.
  - Read and question privacy policies before setup.
- Empower with storytelling: Use poetic or dramatic skits to highlight real-life scenarios—like a student's private moment being recorded or a professional's data being misused.

IV. RESULT

The study reveals that while smart home devices offer convenience and automation, they also introduce significant privacy and security risks. Key findings include:

- Rising User Anxiety: A 2025 Copeland survey shows growing discomfort among users about data collection and surveillance, despite increased adoption of smart home technologies.

- Data Collection Risks: Devices gather extensive personal data—voice, location, behaviour, and biometrics—often without users' full awareness.
- AI-Driven Profiling: AI systems can infer sensitive traits like emotional states or health conditions, raising ethical concerns about manipulation and targeted advertising.
- Security Vulnerabilities: Many devices lack strong security protocols, making them susceptible to hacking, unauthorized access, and data breaches.
- Transparency Issues: Privacy policies are often unclear, leading to uninformed consent and unintentional data sharing.
- Contextual Harms: Students and professionals face unique risks—ranging from surveillance in shared accommodations to data leaks during remote work.

V. CONCLUSION

Smart home ecosystems, while transformative, pose complex privacy and ethical challenges. The research underscores the need for:

- Stronger regulatory frameworks to enforce transparency and data protection.
- User education on privacy settings, consent, and secure usage practices.
- Cross-disciplinary collaboration to design privacy-aware technologies that balance innovation with ethical responsibility.

The paper advocates for a shift from purely technical solutions to holistic strategies that include social awareness, policy reform, and user empowerment—especially in educational and professional environments.

REFERENCE

[1] Lutolf, R. (1992). Smart Home concept.
[2] Lin, H., & Bergmann, N. (2016). IoT security and privacy issues.
[3] Blythe, J., & Johnson, S. D. (2021). Smart home privacy risks.
[4] Tzezana, R. (2016). Biometric data and privacy.
[5] Jacobsson, A., et al. (2016). IoT vulnerabilities.
[6] Nicholls, L., et al. (2020). Cyberstalking and domestic surveillance.
[7] Marikyan, D., et al. (2019). Smart home adoption and challenges.
[8] Nord, J. H., et al. (2019). Trust and stakeholder priorities in IoT.
[9] BEIS (2022). UK smart meter statistics.
[10] Copeland Survey (2025). U.S. homeowner privacy concerns.